CMS/CAIMS Books in Mathematics

Canadian
Mathematical Society
Société mathématique
du Canada

Christian J.-C. Ballot
Hugh C. Williams

The Lucas Sequences

Theory and Applications

Springer

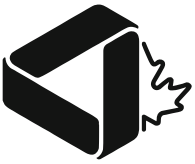
CMS/CAIMS Books in Mathematics

Volume 8

Series Editors
Karl Dilcher, Department of Mathematics and Statistics, Dalhousie University, Halifax, NS, Canada
Frithjof Lutscher, Department of Mathematics, University of Ottawa, Ottawa, ON, Canada
Nilima Nigam, Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada
Keith Taylor, Department of Mathematics and Statistics, Dalhousie University, Halifax, NS, Canada

Associate Editors
Ben Adcock, Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada
Martin Barlow, University of British Columbia, Vancouver, BC, Canada
Heinz H. Bauschke, University of British Columbia, Kelowna, BC, Canada
Matt Davison, Department of Statistical and Actuarial Science, Western University, London, ON, Canada
Leah Keshet, Department of Mathematics, University of British Columbia, Vancouver, BC, Canada
Niky Kamran, Department of Mathematics and Statistics, McGill University, Montreal, QC, Canada
Mikhail Kotchetov, Memorial University of Newfoundland, St. John's, Canada
Raymond J. Spiteri, Department of Computer Science, University of Saskatchewan, Saskatoon, SK, Canada

CMS/CAIMS Books in Mathematics is a collection of monographs and graduate-level textbooks published in cooperation jointly with the Canadian Mathematical Society- Société mathématique du Canada and the Canadian Applied and Industrial Mathematics Society-Société Canadienne de Mathématiques Appliquées et Industrielles. This series offers authors the joint advantage of publishing with two major mathematical societies and with a leading academic publishing company. The series is edited by Karl Dilcher, Frithjof Lutscher, Nilima Nigam, and Keith Taylor. The series publishes high-impact works across the breadth of mathematics and its applications. Books in this series will appeal to all mathematicians, students and established researchers. The series replaces the CMS Books in Mathematics series that successfully published over 45 volumes in 20 years.



Christian J.-C. Ballot • Hugh C. Williams

The Lucas Sequences

Theory and Applications

Springer

Christian J.-C. Ballot
Département de Mathématiques & Informatique
Université de Caen Normandie
Caen, France

Hugh C. Williams
Department of Mathematics & Statistics
University of Calgary
Calgary, AB, Canada

ISSN 2730-650X ISSN 2730-6518 (electronic)
CMS/CAIMS Books in Mathematics
ISBN 978-3-031-37237-7 ISBN 978-3-031-37238-4 (eBook)
https://doi.org/10.1007/978-3-031-37238-4

Mathematics Subject Classification: 11B39, 11-02, 11A51, 11B05, 11B37

© Springer Nature Switzerland AG 2023
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Paper in this product is recyclable.

Dedicated to the memory of John Brillhart (1930–2022), teacher, mentor, friend.

Preface

This book began during a visit of the first author to the second in Calgary in July of 2013. We had both considered separately the possibility of writing a book about the Lucas sequences, but during this visit, we agreed to collaborate on such a project; we also agreed that we were far too busy to begin until several years into the future. The next occasion when we were able to meet was the 18th Conference of the Fibonacci Association in July, 2018, at Halifax, Canada. It was during this meeting that work on this book began in earnest. While we had hoped to complete this undertaking in about 3 years, many obstacles to our progress, not the least of which was the COVID-19 pandemic, prevented its completion until now.

We explain the rationale for this book in the introductory chapter, so we will only mention here that it is the result of a blending of the diverse interests of the authors in various aspects of the Lucas sequences; as such it is a somewhat unusual volume, but we hope it will provide its readers with a good introduction and a sense of the direction of research in this topic. For those readers who wish to delve more deeply into the subject matter, we have attempted to provide a thorough bibliography at the end of each chapter. Unfortunately, it is very possible that we, through inadvertence or ignorance, may not have cited some important contributions; we can only offer our apologies to our readers and the affected authors.

We both have a great interest in the history of mathematics and hope that our readers will forgive our frequent excursions into this area. For those who also appreciate history, we have included an appendix which discusses Édouard Lucas, his times and his work. If he is known at all today, it is usually through his contributions to recreational mathematics, but we hope that this production will illustrate his achievements in other mathematical endeavors, particularly computational number theory.

The origin of Prof. Williams' interest in the Lucas sequences developed from a course in number theory given by Dr. T. M. K. Davison at the University of Waterloo in 1966, while that of Prof. Ballot came from his thesis

work (1990–92) which originated from the study of the 1985 paper of J. Lagarias on the prime divisors of the Lucas numbers. Thus, we have each devoted a substantial portion of our academic careers to their study, an activity which has brought us enormous intellectual and personal satisfaction. It is our hope that the readers of this work will share in our delight in the wonderful properties of these remarkable mathematical objects.

Caen, France — Christian J.-C. Ballot
Ottawa, ON, Canada — Hugh C. Williams
January, 2023

Acknowledgments

Ordinarily, one would expect in this section a list of several names of individuals who have contributed ideas or advice in the creation of this book, but the recent pandemic prevented our attending the professional meetings where we could have discussed this project with knowledgeable experts. However, we were certainly able to use the Internet to acquire many informative publications, and we are most grateful to the authors of these works; their names appear in the bibliographies.

We do wish to thank Andreas Hinz for informing us of the deplorable state of Lucas' grave (with photos) and Andrew Granville for many insightful emails concerning linear division (divisibility) sequences.

We are most grateful to Michael Somos, who generously offered to proofread an earlier version of this book. We also wish to acknowledge the valuable advice of three anonymous reviewers selected by the publisher. Their efforts have resulted in a much improved text. However, it seems inevitable in a work such as this that, in spite of our efforts to eliminate them, some errors or other infelicities will remain. They are the sole responsibility of the authors.

We also point out the willingness of Samuel Hambleton and Jean-Marie De Koninck who shared via emails some of their experience on writing a book in LaTeX, and that of Davy Gigan who directs the computer systems at the University of Caen for his brief but efficient help with some LaTeX issues. Of course, we also thank Suresh Kumar from the Tex-support team at Springer for his patience and polite competent replies.

We also wish to thank Donna Chernyk, Senior Editor (Mathematics) at Springer Science+Business Media, for her assistance in guiding us through the publication process, encouraging our efforts, and for her understanding of several missed deadlines on our part.

Université de Caen — Christian J.-C. Ballot
University of Calgary — Hugh C. Williams
April, 2023

Contents

List of Symbols xv

1 Introduction 1
References 9

2 Basic Theory of the Lucas Sequences 11
2.1 Definition 11
2.2 Most Common Identities 14
2.3 General Divisibility Properties 22
2.4 Divisibility of U_n by Powers of an Odd Prime 27
2.5 Divisibility of U_n by Powers of 2 31
2.6 Composite Integers Dividing U and Their Rank 34
2.7 Divisibility of V_n by Powers of an Odd Prime 35
2.8 Divisibility of V_n by Powers of 2 38
2.9 Composite Integers Dividing V 39
2.10 Euler's Criterion for Lucas Sequences 42
2.11 Degenerate Lucas Sequences 43
2.12 Divisibility by Powers of a Special Prime 45
References 51

3 Applications 53
3.1 Mersenne Primes 53
3.2 Primality Testing 58
3.3 Fast Computation of U_n and $V_n \pmod m$ 63
3.4 Solving Quadratic and Cubic Congruences 65
3.5 Integer Factoring 69
3.6 Diophantine Equations 71
3.7 Cryptography 72
References 74

4 Further Properties ... 79
4.1 Connection with the Circular Functions ... 79
4.2 The Chebyshev and Dickson Polynomials ... 81
4.3 Additional Arithmetic Properties ... 86
4.4 The Lehmer Sequences ... 91
4.5 The Primitive Divisor Theorem ... 93
4.6 Moduli with a Full Set of Residues ... 98
References ... 102

5 Some Properties of Lucasnomials ... 105
5.1 Definition. Connection with q-Binomial Coefficients ... 105
5.2 Integrality ... 107
5.3 Ten Basic Identities ... 110
5.4 Combinatorial Interpretations ... 117
5.4.1 Square-and-Domino-Tiling Interpretations ... 118
5.4.2 An Interpretation Coming from q-Binomial Coefficients 123
5.5 Lucasnomial Catalan Numbers ... 125
5.5.1 Introduction ... 125
5.5.2 Definition and Integrality ... 127
5.5.3 Interpretation of Lucasnomial Catalan Numbers ... 130
5.5.4 The Search for Catalan-Like Triples ... 131
5.6 The p-Adic Valuation of Lucasnomials ... 133
5.6.1 A Generalized Kummer Rule ... 133
5.6.2 A Generalized Legendre Formula ... 137
5.6.3 Explicit Valuations ... 139
5.7 Lucas' Congruence ... 141
5.8 Wolstenholme's Congruence ... 151
5.9 A Word on Lehmernomials ... 158
References ... 160

6 Cubic Extensions of the Lucas Sequences ... 165
6.1 Lucas' Attempts to Generalize His Sequences ... 165
6.2 Cubic Linear Recurrences ... 171
6.3 Bell's Contribution ... 173
6.4 The Cubic Pell Equation ... 174
6.5 Williams's Sequences ... 175
6.6 Roettger's Sequences ... 177
References ... 179

7 Linear Recurrence Sequences and Further Generalizations 183
7.1 Linear Recurrence Sequences ... 183
7.2 Impulse Sequences ... 187
7.3 A Return to the Lehmer Sequences ... 190
7.4 Primality ... 192
References ... 197

8 Divisibility Sequences and Further Generalizations 199
8.1 Another Suggestion of Lucas for Generalizing His Sequences . 199
8.2 Elliptic Divisibility Sequences 201
8.3 Linear Divisibility Sequences 204
8.4 Extended Lucas Sequences 208
8.5 Odd and Even Extensions of the Lucas Sequences 212
References 216

9 Prime Density of Companion Lucas Sequences 219
9.1 How Do We Measure the Size of a Set of Primes? 220
9.2 The Classic Density Theorems 223
9.3 Polynomial Modulo p and Cebotarev 228
9.4 Initial Inquiries of Sierpiński, Brauer, and Ward 234
9.5 The Hasse-Lagarias Method 237
9.6 A Heuristic View 242
9.7 The Laxton Group and Its Generalizations 245
9.7.1 The Laxton Group 245
9.7.2 Generalizations of the Laxton Group 251
9.8 The Density of Maximal Prime Divisors 254
9.9 Irreducible Polynomials Dividing $(X^n + 1)$ 259
References 262

10 Epilogue and Open Problems 267
10.1 Epilogue 267
10.2 Some Unsolved Problems 269
References 277

Appendix: A Short Biography of Lucas 279
References 289

Subject Index 293

Name Index 297

List of Symbols

We present below, in the order in which they appear in the book, several of the most frequently used symbols and the page numbers where they first appear. The reader is cautioned that the same symbol may occasionally be used for two different objects; in these cases, the meaning of the symbol should be clear from context. We first mention that, as is customary, we use $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{F}_q$ to respectively denote the natural, integer, rational, real and complex numbers, and the finite field of q elements. We also use $\gcd(a, b)$ to denote the greatest common divisor of the integers a and b, $\mathrm{lcm}(a, b)$ to denote the least common multiple of a and b, and $\lfloor x \rfloor$ to represent the floor of the real number x, i.e., the largest integer $\leq x$. The fractional part of x is denoted by $\{x\} = x - \lfloor x \rfloor$. Furthermore, we use φ for Euler's totient function.

(X_n), $(X_n)_{n\geq 0}$, X: an ordered sequence of integers: $X_0, X_1, \ldots, X_n, \ldots$, page 1
F_n: the nth Fibonacci number ($F_0 = 0$, $F_1 = 1$), page 1
L_n: the nth Lucas number ($L_0 = 2$, $L_1 = 1$), page 2
α, β: the zeros of the characteristic polynomial $f(x) = x^2 - Px + Q$, page 3
δ: the value of $\alpha - \beta$, page 3
(U_n), (V_n): the Lucas sequences, given by $U_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ and $V_n = \alpha^n + \beta^n$, page 3
$a \mid b$: the integer a divides the integer b, page 12
$\nu_p(r)$: the p-adic valuation of the rational number r, page 12
$p^\nu || n$: the prime power p^ν exactly divides the integer n, page 12
$m \sim_p n$, $m \sim n$ (base p): the integers m and n have the same p-adic valuation, page 12
$[-]$: the Iverson symbol, page 12
$U_n = U_n(P, Q)$, $V_n = V_n(P, Q)$: the Lucas functions, page 12
D: the discriminant of the characteristic polynomial $x^2 - Px + Q$, page 13
$\Psi_n(P, Q)$: polynomial in P and Q associated with U_n, page 19

$\rho(m)$, $\rho_U(m)$: the rank of appearance of the integer m in the Lucas sequence U, page 26
ϵ_p, ϵ_n: respectively, the value of the Legendre symbol $(D \mid p)$ for a given prime p and the value of the Jacobi symbol $(D \mid n)$ for a given odd integer n, page 27
(P_n): the Pell sequence, page 35
$\sigma(m)$, $\sigma_V(m)$: the rank of appearance of the integer m in the Lucas sequence V, page 36
ζ, ζ_n: primitive nth root of unity, page 44
$s(n)$: the sum of the aliquot divisors of the integer n, page 53
M_n: the Mersenne number $2^n - 1$, page 54
$G_m(x)$: the mth Sylvester polynomial, page 64
η_p, η: the value of the Legendre symbol $(Q \mid p)$ for a given prime p, page 68
$\Phi_k(x)$: the kth cyclotomic polynomial, page 70
$T_n(x)$, $U_n(x)$: respectively, the nth Chebyshev polynomials of the first and second kinds, page 82
$C_n(x)$, $S_n(x)$: modified nth Chebyshev polynomials of the first and second kinds, respectively, page 83
$D_n(x, a)$, $E_n(x, a)$: the nth Dickson polynomials of the first and second kinds, respectively, page 85
$\varphi_U(n)$: Lucas' extension of the Euler φ function, page 87
$\mu(n)$: the Möbius function, page 88
Q_n, $Q_n(\alpha, \beta)$: cyclotomic numbers associated with $U_n(P, Q)$, page 89
$\bar{U} = (\bar{U}_n(R, Q), \bar{V}_n(R, Q))$: the Lehmer sequences, page 91
$\omega(m)$: the rank of appearance of the integer m in $\bar{U}$, page 92
sqf (n): the square-free kernel of n, page 94
$\binom{n}{k}_U$: Lucasnomial or Lucasnomial coefficient, page 105
$\binom{n}{k}_F$: Fibonomial or Fibonomial coefficient, page 105
$\binom{n}{k}_q$: the q-binomial coefficient, page 106
$\binom{n}{k}_X$: generalized binomial coefficient, page 107
$\binom{n}{k}_\Psi$: generalized binomial coefficient with respect to the sequence of polynomials (Ψ_n), page 108
$\mathcal{T}_n$: set of tilings of an $1 \times n$ board with squares and dominos, page 118
C_n: the nth Catalan number, page 125
$C_{a,r}(n)$: the nth generalized Fuss-Catalan number, page 126
$C_{U,a,r}(n)$: the nth generalized Lucasnomial Fuss-Catalan number, page 127
$C_{U,a}(n)$: the nth Lucasnomial Fuss-Catalan number, page 127
$C_U(n)$: the nth Lucasnomial Catalan number with respect to U, page 127
$c_q(n)$: the nth Carlitz q-Catalan number, page 128
$C_q(n)$: the nth MacMahon q-Catalan number, page 129
$\mathcal{W}_n$: set of binary words of length $2n$ with at most as many 1's as 0's in any prefix, page 129
maj(w): the major index of the binary word w, page 129
$m!_U$: $U_m U_{m-1} \cdots U_1$, the factorial of m with respect to U, page 135

$[x^t]f(x)$: coefficient of x^t in the polynomial $f(x)$, page 142

$M(p)$: the multiplier of the prime p with respect to a Lucas sequence U, page 149

$\binom{n}{k}_{\bar{U}}$: Lehmernomial or Lehmernomial coefficient, page 158

(x_n), (y_n), (z_n): Bell's sequences, page 173

ρ_i $(i = 1, 2, \ldots, k)$: the k zeros of $f(x)$, page 174

(X_n): any integer sequence which satisfies the kth order linear recurrence

$$X_{n+k} = P_1 X_{n+k-1} - P_2 X_{n+k-2} + \cdots + (-1)^{k-1} P_k X_n,$$

where P_1, P_2, ..., P_k are given fixed integers and $T_0 = (X_0, X_1, \ldots, X_{k-1})$ is a fixed initial vector of k integer values, page 184

$(Z_{i,n})$: the above (X_n) for each $i = 0, 1, 2, \ldots, k-1$, and $Z_{i,j} = \delta_{i,j}$, $(0 \le i, j < k)$, where $\delta_{i,j} = 0$ when $i \neq j$ and $\delta_{i,i} = 1$, page 174

(W_n), (V_n), (U_n), (R_n), (S_n), (T_n): Williams's sequences, page 176

(W_n), (U_n): Roettger's sequences, page 178

$f(x)$: the characteristic polynomial of (X_n), page 184

$\tau(m)$: the minimal period length of the above (X_n) modulo the integer m, page 184

(Z_n): the above (X_n) with $T_0 = (0, 0, 0, \ldots, 0, 1)$, i.e., $Z_n = Z_{k-1,n}$, page 185

$\pi(m)$: the minimal period length of (Z_n) modulo the integer m, page 185

Δ: the discriminant of $f(x)$, page 187

α_i, β_i $(i = 1, \ldots, k)$: the values satisfying $\alpha_i + \beta_i = \rho_i$, $\alpha_i \beta_i = Q$, page 190

$(U_{i,n})$, $(V_{i,n})$, $(i = 0, 1, 2, \ldots, k-1)$: the generalized Lehmer sequences, page 190

$F(x)$: the characteristic polynomial of the generalized Lehmer sequences, page 191

D: the discriminant of $F(x)$, page 191

$\mathcal{A}_n$, $\mathcal{C}_n$: $\mathcal{A}_n = \gcd(U_{0,n}, U_{1,n}, \ldots, U_{k-1,n})$ and, when $k > 1$, $\mathcal{C}_n = \gcd(V_{1,n}, V_{2,n}, \ldots, V_{k-1,n})$, page 192

(W_n): Ward's elliptic divisibility sequence, page 202

(Δ_n), (S_n): Pierce's sequences, page 209

(U_n), (V_n): generalizations of Pierce's sequences, page 209

(X_n): an integer sequence with characteristic polynomial $F(x)$. If $X_{-n} = Q^{-n} X_n$ for all integral n, (X_n) is said to be even; if $X_{-n} = -Q^{-n} X_n$ for all integral n, (X_n) is said to be odd, page 212

$(p_n)_{n \ge 1}$: the ordered sequence of all (rational) prime numbers with $p_1 = 2 < p_2 = 3 < \ldots$, page 220

$\mathcal{P}$: the set of all rational primes, page 220

$d = d(S)$: the natural density of a set of primes $S \subset \mathcal{P}$, page 221

$\delta(S)$: the logarithmic density of a set of primes S, page 222

$\mathcal{O}_K$: the ring of algebraic integers in a number field K, page 224

$f = f(P \mid p)$: the inertial degree of a prime ideal P over the rational prime p, page 225

$D = D(Q \mid P)$: the decomposition group of Q over P, page 225

$\Phi = \Phi(Q \mid P)$: the Frobenius automorphism relative to P and Q, page 226
$C_p(K/\mathbb{Q})$: the conjugacy class of $\Phi(P \mid p)$, P prime ideal above p in $\mathcal{O}_K$, page 226
$m_\alpha(x)$: the minimal polynomial of the algebraic integer α, page 227
d_i: the density of primes p for which $f(x)$ admits exactly i zeros modulo p, page 230
$F(g)$: In the action of a group G on a set X, the number of points $x \in X$ such that $g \cdot x = x$, $(g \in G)$, page 231
Z_i: subset of the elements of the Galois group of $f(x)$ which fix exactly i zeros of $f(x)$, page 231
S: the Stephens constant, page 242
$F(f)$: semigroup structure on the set of linear recurrences with the same characteristic polynomial f of degree 2, page 245
$G(f)$: the Laxton group derived from $F(f)$, page 245
$T(f)$: the torsion subgroup of $G(f)$, page 246
$\rho_{\max}(p)$: rank of maximal division of the prime p with respect to some fundamental recurrence U of order $m \geq 2$, page 252
C_n: the nth Cullen number $n2^n + 1$, page 253
$C_f(n)$: the nth generalized Cullen number, page 253

Chapter 1
Introduction

The secret of getting ahead is getting started. (Mark Twain)

In his youth Albert Einstein spent a year loafing aimlessly. You don't get anywhere by not 'wasting time.' (Carlo Rovelli)

As this is a book about number sequences, we begin by defining a number sequence to be an ordered set of numbers. We will often use the notation (X_n) or sometimes simply X to denote the sequence $X_0, X_1, X_2, \ldots, X_n, \ldots$ This will be convenient because we will be dealing with recurrence sequences whose elements are related to the previous elements in a clear-cut way. To define such a sequence, we require a rule, called a recurrence relation, to construct each element in terms of the ones before it. Furthermore, enough initial elements must be given so that all subsequent elements of the sequence can be computed by successive applications of the recurrence relation. For example, consider the *Fibonacci numbers*. These numbers are defined by the initial elements $F_0 = 0$ and $F_1 = 1$ and the recursion formula $F_{n+1} = F_n + F_{n-1}$, for $n \geq 1$. The sequence is thus $0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$ However, since $F_{n-1} = F_{n+1} - F_n$, we can compute $F_{-1} = -1, F_{-2} = 1, F_{-3} = -2, \ldots, F_{-n} = (-1)^n F_n$. Thus, the complete Fibonacci sequence is

$$\ldots 21, -13, 8, -5, 3, -2, 1, -1, 0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$$

Since many of the sequences that we will discuss can be extended in this way, we will occasionally use the notation (X_n) to represent the full sequence

$$\ldots, X_{-n}, \ldots, X_{-2}, X_{-1}, X_0, X_1, X_2, \ldots, X_n, \ldots .$$

It should be clear from the context which sequence is meant.

© Springer Nature Switzerland AG 2023

C. J.-C. Ballot, H. C. Williams, *The Lucas Sequences*, CMS/CAIMS Books in Mathematics 8, https://doi.org/10.1007/978-3-031-37238-4_1

Perhaps as early as 1202, the Fibonacci numbers were presented by Leonardo Bonacci in his *Liber Abbaci* (*Book of Calculation*)[†], as the solution of a problem of computing the number of rabbits that would result at time n under a particular breeding model. Certainly, we know that they appeared in the 1228 edition of this book. Leonardo (c. 1170–c. 1240–1250), a thirteenth-century Pisan mathematician, was known by other names such as Leonardo Pisano and Leonardo Bigollo (Pisano), but he is best known today as Fibonacci, a contraction of filius Bonacci (son of Bonacci), invented by the French historian Guillaume Libri in 1838. (See Devlin [5] for more details concerning what little is known about Fibonacci.) We emphasize here that Fibonacci was not the first to discuss these numbers; they were known much earlier to Indian mathematicians. (See Singh [25].) Because of their intrinsic interest and their many applications, the Fibonacci numbers have been the object of a considerable body of research; indeed, an entire journal, the *Fibonacci Quarterly*, established in 1963, is devoted to the study of their many properties and those of recurrence sequences in general. In addition, we mention the books of Gilson [8], Koshy [11], Posamentier and Lehman [22], and Vajda [27], each of which is dedicated to the study of the Fibonacci and Lucas numbers. The sequence of *Lucas numbers* (L_n) satisfies the same recurrence relation as the Fibonacci numbers, but with initial terms $L_0 = 2$ and $L_1 = 1$.[‡] The sequences (F_n) and (L_n) possess a variety of properties, many of which can be found in the encyclopedic [11]. We mention here that (L_n) has even found an application in dynamical systems. See Puri and Ward [23], where it is shown that the only recurrence sequence satisfying the Fibonacci recurrence and realizable as the number of periodic points of a map must be a multiple of (L_n).

A very notable feature of the Fibonacci numbers is the number of algebraic identities that they satisfy. For example, consider the identity discovered in 1680 by G. D. Cassini [11, pp. 85–86, 106, 114]:

$$F_n^2 - F_{n+1}F_{n-1} = (-1)^{n-1};$$

this is a special case of the identity of Catalan

$$F_n^2 - F_{n+m}F_{n-m} = (-1)^{n-m}F_m^2,$$

which in turn is a special case of Vajda's [27, (20a)] identity:

$$F_nF_{n+i-j} - F_{n+i}F_{n-j} = (-1)^{n-j}F_iF_j.$$

A yet more general and more symmetric form can be found in Johnson [10]:

[†] The *Liber Abbaci* was first published in 1202, but no copies of this version of the book have survived. Several copies of the second 1228 edition, however, are extant. (See [5].)

[‡] The term "Lucas numbers" for the numbers $2, 1, 3, 4, 7, 11, \ldots$ seems to have become more and more common in the mid-1960s in papers published in the *Fibonacci Quarterly*.

$$F_aF_b - F_cF_d = (-1)^r(F_{a-r}F_{b-r} - F_{c-r}F_{d-r}),$$

as long as $a + b = c + d$. Put $a = n$, $b = n + i - j$, $c = n + i$, $d = n - j$, and $r = n - j$ to obtain Vajda's identity. As can be seen in [11], there are many, many more identities involving the (F_n) and (L_n) sequences.

By computing a table of the Fibonacci numbers and their corresponding prime divisors, Lucas was able to discover empirically several characteristics of these factors [28, Sect. 3.1], which he was later able to prove in [16]. Indeed, it is now known that the Fibonacci numbers possess a large number and variety of fascinating number-theoretic properties.

In 1844, Gabriel Lamé [12], in his quest to bound the number of divisions needed in executing the Euclidean algorithm for determining the greatest common divisor of two integers, rediscovered the Fibonacci numbers. Up to 1876, the Fibonacci sequence was known to Lucas as the Lamé sequence (or the Lamé series). In January of 1876, Lucas [14] published a most remarkable short paper (actually, an extended abstract), in which he determined the possible linear forms of primes which divide certain elements of the Lamé (Fibonacci) sequence, the Lucas numbers, originally defined as F_{2n}/F_n and denoted now by L_n. He mentioned the identities $L_{n+1} = L_n + L_{n-1}$ and $L_{2n} = L_n^2 - 2(-1)^n$ and concluded the paper with the following (at that time) astonishing statement:

> Furthermore, it is important to remark that Theorems X and XI allow us to determine whether a number is prime or composite without making use of a table of prime numbers. It is with the aid of these theorems that I think I have proved that the number $A = 2^{127} - 1$ is prime. This number consists of *thirty-nine* digits, while the largest prime number currently known consists of only ten digits. This number is, according to Euler, equal to $2^{31} - 1$.

The aforementioned Theorems X and XI are stated without proof in the paper. Also, the largest prime known in 1876, but not to Lucas, was in fact a number of 14 digits (see Chap. 2 of Williams [28]), but the statement that he could prove A to be a prime was quite extraordinary because at the time, the number was considered to be very large. Certainly, proving A a prime by trial division would have been out of the question; indeed, it remained the largest known prime for another 75 years.

In May of 1876, Lucas [15] introduced the sequences that would later bear his name. He let P and Q be coprime integers and α and β be the roots of the quadratic polynomial $f(x) = x^2 - Px + Q$ with $\delta = \alpha - \beta$. He then defined what are now called the *Lucas sequences* (U_n) and (V_n) by using the functions

$$U_n = (\alpha^n - \beta^n)/\delta, \quad V_n = \alpha^n + \beta^n.$$

Since both U_n and V_n are symmetric functions of the roots of a polynomial with integer coefficients, they must both be integers for all nonnegative integral values of n. He stated that when $P = 1$ and $Q = -1$, then U_n and V_n are, respectively, the corresponding Fibonacci and the Lucas numbers. He

also listed a number of identities, including a generalization of the Cassini identity:

$$U_n^2 - U_{n+1}U_{n-1} = Q^{n-1}.$$

It was in this paper that he pointed out that the sequence of Lamé had been discovered much earlier by Fibonacci. It has been called the Fibonacci sequence ever since, in spite of the priority of the Indian mathematicians of whose work Lucas was completely unaware.

On reading [15], Genocchi [7] pointed out that Lucas' functions were very similar to a pair of functions that he [6] had introduced several years earlier. Genocchi had anticipated several of Lucas' findings and mentioned that versions of his functions were known to Lagrange and Legendre. Nevertheless, because of the enormous number and variety of results involving (U_n) and (V_n) that Lucas discovered from 1876 until about 1880, they are now named after him. In fact, it was during this period that he applied them in developing tests for the primality of large integers, including what is now called the Lucas-Lehmer test for the primality of Mersenne numbers. For the most part, these tests were sufficiency tests, which, if they were satisfied, could establish that a number N of a certain special form is a prime. As Lucas well realized, these tests were quite novel for their time, because instead of having to trial divide N by a large number of integers, for example, all the primes less than $\sqrt{N}$, it was only necessary to compute some integer S and test whether N divides S.

As it seems that Lucas was unaware of the previous work of Genocchi, Lagrange, and Legendre, it is of some interest to investigate where the idea of his functions arose. He does not really address this in [15], instead emphasizing the similarity between his functions and the trigonometric circular functions (see Sect. 4.1). As early as 1872, undoubtedly as a result of his examination of the works of Fermat, he had sharpened his interest in Diophantine problems. (See Lucas [13, 16, 18], where the problems in [13] are dealt with more extensively.) He was almost certainly aware at this time of "Fermat's last theorem" (FLT). Indeed, much later (1891) in [20], he states:

> We had hoped to find in this study [of the Lucas sequences], through the prime decomposition of the expressions $(a^n \pm b^n)$, a demonstration of Fermat's last theorem concerning the impossibility of solving in integers the indeterminate equation
>
> $$x^p + y^p + z^p = 0$$
>
> in which it suffices to assume that p denotes a prime.

Thus, it appears that attempting to prove FLT was a motivating force behind his invention of the Lucas sequences and the development of their theory, but so also was his application of them in primality testing (see Sect. 3.1). Additional information concerning this matter can also be found in Sect. 6.1. It seems remarkable that Lucas did not mention anything about this in print until near the end of his truncated life (see the Appendix), but possibly he

was concerned about not revealing too much information until he had solved the problem or saving himself the embarrassment of failing to do so. In connection with this, it is a great pity that his early death prevented him from completing, among other projects, his proposed commentary on the works of Fermat, which he mentions on page vi of [19] and on the last page of [18].

Although much has been written about the Fibonacci and Lucas numbers, no monograph devoted to the properties of the Lucas sequences has ever appeared in print. This seems remarkable in view of the fact that almost all results concerning the Fibonacci and Lucas numbers have Lucas sequence analogues. There are, however, a few books, besides elementary textbooks, which include substantial sections dedicated to these sequences, particularly as they apply to primality testing. Some of these are Bressoud and Wagon [3], Crandall and Pomerance [4], Ribenboim [24], and Williams [28].

The objective of this book is to provide a much more thorough discussion of the Lucas sequences than is available in existing monographs. We will bring together a variety of results, which are currently scattered throughout the literature. Various sections will be devoted to intrinsic arithmetic properties of these sequences, primality testing, density problems, and the problem of generalizing them. Furthermore, their application, not only to primality testing but to integer factoring, solution of quadratic and cubic congruences, cryptography, and Diophantine equations, will be briefly discussed. Throughout the book, we will include a sprinkling of historical comments, where relevant.

Much of the book is not intended to be overly detailed. Rather, our objective is to provide a good, elementary, and clear explanation of the subject matter without too much ancillary material. Most chapters, with the exception of the second and the fourth, will address a particular theme, provide enough information for the reader to get a feel for the subject, and supply references to more comprehensive results. We have also attempted to make most of this work accessible to anyone with a basic knowledge of elementary number theory and abstract algebra. Our intended audience is number theorists, both professional and amateur, students, and enthusiasts. We emphasize that this book was never intended to be a textbook; its focus is either much too narrow or too broad for that, but it might be used as supplementary reading for students enrolled in second or more advanced courses in number theory.

Lucas sequences are very simple mathematical objects. They are sequences of integers, where each term of the (U_n) or the (V_n) sequence is a fixed weighted sum of the two previous terms. That is, for all n, we have

$$X_{n+2} = PX_{n+1} - QX_n,$$

where X is a U or a V Lucas sequence. One would naturally expect them to have mainly additive properties. However, many of their key features arise from their divisibility properties. Several chapters of this book, in one manner or another, show or exploit themes rooted in the multiplicative nature of these sequences. For example, U_m is a multiple of U_n whenever m is a multiple of

n, if m and n are positive integers. We saw that the celebrated Fibonacci sequence and its companion sequence, the sequence of Lucas numbers, form one instance of a pair of Lucas' functions for $P = 1$ and $Q = -1$. But putting $P = 2$ and $Q = 1$ yields $U_n = n$ and $V_n = 2$ for all n. This observation, i.e., the fact that the sequence of natural numbers is a Lucas sequence, has been an abundant source of discovery of properties of the Lucas sequences and probably still holds many more future findings. We may call this phenomenon the $n \to U_n$ theme. For instance, the simple remarkable identity $2n + 1 = (n + 1)^2 - n^2$, which has the Fibonacci cousin identity $F_{2n+1} = F_{n+1}^2 + F_n^2$, generalizes to $U_{2n+1} = U_{n+1}^2 - QU_n^2$, for an arbitrary Lucas sequence $U(P, Q)$. The trivial identity $(2n) = 2 \cdot n$ generalizes to $U_{2n} = V_n \cdot U_n$ for a generic pair (U, V) of Lucas sequences. In the 1860s, Wolstenholme discovered that given a prime $p \geq 5$, if we express the rational number $\sum_{n=1}^{p-1} 1/n$, in lowest terms as A/B, A and B natural numbers, then A is a multiple of p^2. Clearly, the sum $\sum_{n=1}^{p-1} 2/n$ has the same property and is a particular instance of the more general sum $\sum_{n=1}^{\rho-1} V_n/U_n$, where the rank ρ of the prime p in the Lucas sequence (U_n) is the least positive index t for which $p \mid U_t$. Remarkably, if ρ is p or $p \pm 1$, then the numerator of the rational number $\sum_{n=1}^{\rho-1} V_n/U_n$ is a multiple of p^2, $(p \geq 5)$. We illustrate the $n \to U_n$ theme with two more examples.

Two (disjoint) products of consecutive positive integers (containing each at least two terms) are never equal except in one instance. At least one direction of the statement is easily checked. Indeed,

$$14 \cdot 15 = 5 \cdot 6 \cdot 7, \tag{1.1}$$

and both products are 210. Thus, one is led to investigate the corresponding question in the context of a general Lucas sequence U. Given two nonzero integers P and Q and $U = U(P, Q)$, solve the Diophantine equation

$$U_m U_{m+1} \cdots U_{m+s} = U_n U_{n+1} \cdots U_{n+t}, \tag{1.2}$$

in positive integers m, n, s, and t, with s and t at least two. Corollary 1.3 and Table 1 p. 293 of [26] tell us, among other things, that no other solutions to (1.2) exist, besides (1.1).

An integer sequence X has the *Pillai property* if there is a (minimal) bound $b_X \geq 2$ such that for all $k \geq b_X$, the sequence X has k consecutive terms such that none is prime to the product of the $k-1$ others. The sequence of natural numbers I, $(I_n = n)$, is a Pillai sequence with $b_I = 17$. (See [2, 21].) Hajdu and Szikszai proved [9, Thm. 1] that every *nondegenerate* Lucas sequence $U(P, Q)$, i.e., such that $U_n \neq 0$ if $n \geq 1$, satisfying $\gcd(P, Q) = 1$, is a Pillai sequence. For most parameters P and Q, b_U is again equal to 17, but there are two infinite families of parameters (P, Q) with, respectively, $b_U = 25$ and $b_U = 43$. For the Fibonacci sequence, $b_F = 25$.

The two foregoing topics, and a number of other results concerning Lucas sequences, are not treated in this book. This is to say that, although this book gathers together the basic theory of Lucas sequences and certain special topics, applied and theoretical, that are dear to the authors, it was not our intention to give an exhaustive account of the subject, much of which can be found in number theory journals, and in particular, but not exclusively, in *Integers*, the *Fibonacci Quarterly*, and the *Journal of Integer Sequences*, all of which provide a free online access to their papers, with a modest current Fibonacci fee (i.e., \$55 or \$89) for access to the last 5 years of the *Fibonacci Quarterly*.

We begin, in the next chapter, by providing a thorough and rigorous account of the basic identity and arithmetic features of the Lucas sequences summarized in Lucas' memoir [17]. We will not, however, record a great many of the large number of identity properties involving (U_n) and (V_n) that Lucas discovered—only the ones that we found useful in the development of our theme. For those who are interested in identities, we refer the reader to [17] and Chap. 4 of [28]. Many more identities can be found in various articles of the *Fibonacci Quarterly*, but also in the *Journal of Integer Sequences* or in *Integers*, and to a lesser degree in the *Journal of Number Theory* and the *International Journal of Number Theory*. For example, the first formula of [28, (4.2.4)] is the Lucas function version of Catalan's identity:

$$U_n^2 - U_{n+m}U_{n-m} = Q^{n-m}U_m^2,$$

an identity which occurs as (32) in [17]. Also, [28, (4.2.14)] yields the Lucasian analogue of Vajda's formula:

$$U_nU_{n+i-j} - U_{n+i}U_{n-j} = Q^{n-j}U_iU_j.$$

A short proof of the Lucasian analogue of Johnson's formula can be found in [1, Lemma 6]:

$$U_aU_b - U_cU_d = Q^r(U_{a-r}U_{b-r} - U_{c-r}U_{d-r}),$$

which holds provided $a + b = c + d$.

Furthermore, we do not always insist that $\gcd(P, Q) = 1$. Some of the results that we will mention, particularly the divisibility properties of V_n, seem not to have been known to Lucas, but it is difficult to know this for certain because he stated in [18, p. 44] that he had produced an additional 20 sections for [17] which he had not yet published (and never did).

In Chap. 3, we start with a discussion of the Mersenne numbers. We next describe several applications of the Lucas sequences to such problems as primality testing, solving certain congruences modulo a prime, and integer factorization. We then look at how these sequences have been used to deal with some particular Diophantine equations and with the problem of secure

communication. As in any of these applications, it is essential that we be able to compute remote terms in the Lucas sequences modulo some fixed number; we show how this can be done efficiently.

Chapter 4 consists of several miscellaneous results concerning the Lucas sequences. These include the relationship of these sequences to the circular functions, the Chebyshev polynomials, and the Dickson polynomials. We also provide some further arithmetic properties of the Lucas sequences, briefly describe Lehmer's extension of these sequences, and discuss the primitive divisor theorem. We conclude by considering the problem of finding those moduli for which (U_n) has a full set of residues.

Chapter 5 is an in-depth examination of the Lucasnomials and their properties. These objects, which can be considered as generalizations of the binomial coefficients, owe their integrality to a remark made by Lucas, but beyond that, he did not provide results concerning them.

Chapters 6, 7, and 8 are devoted to various aspects of Lucas' problem of finding a generalization of his sequences. Several of Lucas' ideas are discussed at some length, and some candidates as possible generalizations are provided.

Every prime number not dividing Q divides some of the terms U_n. However, if infinitely many primes divide terms of a given V sequence, infinitely many do not. Chapter 9 explains how starting with initial questions asked independently by Sierpiński for (2^n+1) and by Ward for (L_n), Hasse, and later Lagarias came up with a remarkable method that gives the exact proportion of primes that divide a V sequence. For instance, on average, 17 out of 24 primes divide some term of the form 2^n+1. A generalization of the method of Hasse and Lagarias to computing the density of primes which divide $s-1$ consecutive terms for some specific linear recurrences of order s, $(s \geq 2)$, is also explained.

In Chap. 10, we provide a brief overview of the book and a selection of unsolved problems or open investigations.

Finally, in the Appendix, we provide a short biography of Lucas' life, where we mention some of his personality traits and discuss his legacy.

Every chapter starts with some quotations. They should be viewed as condiments to the main text. We have limited ourselves to realms that may supposedly be of interest to our readership. Many of us teach and, thus, have to communicate effectively; many do research and many enjoy mathematics; others yet are students of mathematics. Consequently, these passages apply to mathematics, the sciences, research, creativity, the learning process, writing, telling, teaching, communication, perseverance, intuition, and even poetry. Partially in honor of Édouard Lucas, we have often elected not to translate quotations from French authors into English.

References

1. C. Ballot, *Another Lucasnomial Generalization of Wolstenholme's Congruence*, J. Integer Seq. **23** (2020), Article 20.3.7.
2. A. Brauer, *On a property of k consecutive integers*, Bull. Amer. Math. Soc. **47** (1941), 328–331.
3. David Bressoud and Stan Wagon, *A Course in Computational Number Theory*, Key College Publishing, 2000, 367pp.
4. Richard Crandall and Carl Pomerance, *Prime Numbers: A Computational Perspective*, 2nd Edition, Springer, 2005, 597pp.
5. Keith Devlin, *Finding Fibonacci*, Princeton University Press, Princeton NJ, 2017.
6. A. Genocchi, *Intorno ad alcune forme di numeri primi*, Annali Mat. Pura Appl. **2**(2) (1868/9), 256–267.
7. A. Genocchi, *Intorno a tre problem aritmetici*, Atti della Reale Accademia della Scienze di Torino **11** (1876), 811–829, Addendum 924–927.
8. B. R. Gilson, *The Fibonacci Sequence and Beyond*, CreateSpace, 2009, 146pp.
9. L. Hajdu and M. Szikszai, *On the GCD-s of k consecutive terms of Lucas sequences*, J. Number Theory **132** (2012), no. 12, 3056–3069.
10. Robert C. Johnson, *Fibonacci numbers and matrices*, preprint, 2009, available with the author's permission at https://www.researchgate.net/publication/228548460_Fibonacci_numbers_and_matrices.
11. Thomas Koshy, *Fibonacci and Lucas Numbers with Applications*, Vol. 1, Second ed., John Wiley and Sons, 2018, 669pp.
12. G. Lamé, *Note sur la limite du nombre des divisions dans la recherche du plus grand commun diviseur entre deux nombres entiers*, C. R. Acad. Sci. Paris Sér. I Math. **19** (1844), 867–870.
13. É. Lucas, *Recherches sur l'analyse indéterminée et arithmétique de Diophante*, Bulletin de la Société d'émulation du Département de l'Allier **12** (1873), 441–532.
14. É. Lucas, *Note sur l'application des séries récurrentes à la recherche de la loi de distribution des nombres premiers*, C. R. Acad. Sci. Paris Sér. I Math. **82** (1876), 165–167.
15. É. Lucas, *Sur la théorie des nombres premiers*, Atti della Reale Accademia della Scienze di Torino **11** (1876), 928–937.
16. É. Lucas, *Recherches sur plusieurs ouvrages de Leonardo de Pise et sur diverses questions d'arithmétique supérieure*, Bolletino di Bibliografia e di Storia della Scienze Matematiche e Fisiche **10** (1877), 129–193, 239–293.
17. É. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. of Math. **1** (1878), 184–240, 289–321.
18. É. Lucas, *Notice sur les Titres et Travaux Scientifiques de M. Édouard Lucas*, D. Jouaust, Paris, 1880.
19. É. Lucas, *Récréations Mathématiques*, Deuxième édition, Gauthier-Villars, Paris, 1891.

20. É. Lucas, *Questions proposées à la discussion des 1re et 2e sections, 1° Questions d'arithmétique supérieure*, Assoc. Française pour l'Avancement des Sciences, Compte rendu des sessions **20** (1891), 149–151.
21. S. S. Pillai, *On m consecutive integers*, I. Proc. Indian Acad. Sci., Sect. A. **11** (1940), 6–12.
22. A. S. Posamentier and I. Lehman, *The Fabulous Fibonacci Numbers*, Prometheus Books, 2007, 364pp.
23. Y. Puri and T. Ward, *A dynamical property unique to the Lucas sequence*, Fibonacci Quart. **39** (2001), no. 5, 398–402.
24. Paulo Ribenboim, *The Book of Prime Number Records*, 2nd Edition, Springer-Verlag, 1989, 479pp.
25. P. Singh, *The so-called Fibonacci numbers in ancient and medieval India*, Historia Mathematica **12** (1985), 229–244.
26. M. Szikszai, *Distinct products in Lucas sequences–on a problem of Kimberling*, Fibonacci Quart. **55** (2017), no. 4, 291–296.
27. S. Vajda, *Fibonacci and Lucas Numbers, and the Golden Section: Theory and Applications*, Dover Publications, Inc., 2008.
28. H. C. Williams, *Édouard Lucas and Primality Testing*, Wiley-Interscience, John Wiley and Sons, New York, 1998.

Chapter 2
Basic Theory of the Lucas Sequences

A mathematician is a pattern searcher. That's all we do all day.
(Marcus de Sautoy)

Understanding is a kind of ecstasy. (Carl Sagan)

Abstract This chapter discusses the fundamental properties of Lucas sequences. Those who have worked with, or who have had an interest in, Lucas sequences will be aware of a good part of the material in the chapter, but we hope to bring about a degree of precision and completeness concerning these basic properties along with proofs. Regular, standard, degenerate, as well as general Lucas sequences are defined. Their most basic and important identities are reviewed; divisibility properties and the p-adic valuation of their terms are studied for all primes p, whether regular or special. The notion of the rank and rank exponent of a prime, the Lucas laws of appearance and repetition, the lifting-the-exponent lemma, as well as the Euler criterion for Lucas sequences are encountered along the way. We did not seek the most concise exposition, but rather one that brings some insight and is strewn with remarks. In fact, we often give several proofs of the same result, providing elementary ones always, but occasionally also proofs that use basic algebraic number-theoretic concepts. Of course, these results are of use, in particular, in all chapters of the book.

2.1 Definition

The theory and properties of the Lucas sequences are scattered in various places in the literature and were already largely present in Lucas' work [12, 13], although not expressed as clearly as by later authors (Carmichael [3], D. H. Lehmer [10], etc.) or by those who, here and there, taught classes

© Springer Nature Switzerland AG 2023

C. J.-C. Ballot, H. C. Williams, *The Lucas Sequences*, CMS/CAIMS Books in Mathematics 8, https://doi.org/10.1007/978-3-031-37238-4_2

in number theory that included this subject. For instance, Raphael Robinson took classes from D. N. Lehmer at the University of California at Berkeley which included some theory of Lucas sequences. The theory of Lucas sequences was taught by Robinson himself in the 1950s at the same university. John Brillhart, who attended Robinson's lectures, taught such a class at the University of Arizona in the fall of 1993, which one of the authors of this book had the opportunity to attend. Part of the basic theory of Lucas sequences has also appeared elsewhere more recently: in two sections of the book of Hardy and Wright [7, Sect. 10.14; Sect. 15.5], in Ribenboim's original paper [15], in Williams' book [17, Chap. 4], and in Ballot's paper [1]. The p-adic valuation of terms of the Lucas sequences treated here in Sects. 2.4, 2.5, 2.6, and 2.7 has appeared in [11] for the Fibonacci and Lucas numbers, in [1, Sect. 3.2.1], in [17, Chap. 4], and even more recently in [16]. But some material has either seldom or never appeared in published form yet, particularly in Sects. 2.9 and 2.12.

We emphasize some notation used in the chapter. If a and b are rational integers, we say that a divides b and write $a \mid b$, provided there is a rational integer c such that $b = ac$. In particular, $0 \mid a$ implies $a = 0$. Given a rational prime p and an integer n, its p-adic valuation, $\nu_p(n)$, is the largest nonnegative integer v such that $p^v \mid n$. Thus, $p^{v+1} \nmid n$. We put $\nu_p(0) = +\infty$. We also write $p^v \,||\, n$. If m/n is a rational number, then its p-valuation is the valuation difference $\nu_p(m) - \nu_p(n)$. Thus, $\nu_2(-24) = 3$, $\nu_3(2/9) = -2$, and $\nu_5(7/6) = 0$. Within the rational integers $\mathbb{Z}$, the relation $m \sim_p n$, or $m \sim n$ (base p), says that the integers m and n have the same p-adic valuation. Hence, $3 \sim_3 42$, $2 \sim_3 1$, and $75 \sim 25 \pmod 5$. If $n \sim_p 0$, then $n = 0$. We make frequent use of the Iverson symbol $[-]$, which is the Boolean function that assigns 1 to $[\mathcal{P}]$, if $\mathcal{P}$ is a true statement, and 0, if $\mathcal{P}$ is false.

Given two nonzero rational integers P and Q, one defines a pair $\{U, V\}$ of Lucas sequences. They both satisfy the same binary recursion

$$X_{n+2} = PX_{n+1} - QX_n, \text{ for } n \geq 0. \tag{2.1}$$

One is called the *fundamental* Lucas sequence. The other is the *companion*, or the *associate* Lucas sequence. Following Lucas and tradition, $U(P, Q)$, or more briefly the letter U, denotes the fundamental sequence, while $V(P, Q)$, or V, denotes the companion sequence. The sequence $U = (U_n)_{n\geq 0}$ satisfies the initial conditions

$$U_0 = 0,\ U_1 = 1. \tag{2.2}$$

The initial conditions that define the companion sequence are

$$V_0 = 2,\ V_1 = P. \tag{2.3}$$

Note that all terms U_n and V_n, $n \geq 0$, are integral. We often refer to $U_n = U_n(P, Q)$ and $V_n = V_n(P, Q)$ as the *Lucas functions*. In the interest of brevity, we will often use the symbols U_n and V_n without including the parameters

P and Q when it is understood from context what P and Q are or when we refer to $U_n(P, Q)$ and $V_n(P, Q)$ for any P and Q.

Lucas and, subsequently, many authors developed the theory with the hypothesis that the parameters P and Q are coprime. The Lucas sequences are said to be *regular* whenever $\gcd(P, Q) = 1$. Although regular Lucas sequences possess stronger properties, we do not generally choose this approach because much of the Lucas theory remains valid, or "locally" valid for primes p not dividing $\gcd(P, Q)$, for nonregular sequences. In fact, the mathematical literature contains many papers that prove results about regular Lucas sequences, which hold just as well for nonregular Lucas sequences.

We let $D = P^2 - 4Q$ denote the discriminant of the characteristic polynomial $x^2 - Px + Q$ and α and β denote its zeros.[†] Thus, $D = (\alpha - \beta)^2$, $P = \alpha + \beta$, and $Q = \alpha\beta$. Throughout this work, we will write δ for $\alpha - \beta$ so that

$$\alpha = \frac{P + \delta}{2} \quad \text{and} \quad \beta = \frac{P - \delta}{2}. \tag{2.4}$$

(The usual convention when $D > 0$ is to choose $\alpha > \beta$.)

If $D \neq 0$, then the closed forms of U_n and V_n, their so-called Binet form, symmetric in the two zeros, are

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad V_n = \alpha^n + \beta^n. \tag{2.5}$$

Remark 1 Thus, the integrality of all U_n terms, $n \geq 0$, generalizes the fact that for all rational integers x and y, $x - y$ divides $x^n - y^n$.

Remark 2 One sees that the fundamental sequence is, up to a constant, the difference of two exponential functions, while the companion is the sum of these two same functions. The sine and the cosine functions, respectively, obey the same property. This explains the title of the famous memoir of Lucas [12]. As Lucas had observed [12, Sect. II], this remark provides an explanation for the existence of a correspondence between trigonometric identities, or hyperbolic identities, and the Lucas identities involving the sequences U and V. In some substantial way, the arithmetic of a Lucas pair $\{U, V\}$ constitutes a discrete version of trigonometry.

For some results, it is either necessary or convenient to assume that all terms U_n, $n \geq 1$, are nonzero. Such sequences are said to be *nondegenerate*. On the contrary, if some $U_n = 0$ with $n \geq 3$, then U is called *degenerate*. A complete description of degenerate cases is done in Sect. 2.11. Had we allowed the parameter P to be 0, all our theory would have carried over; but if $P = 0$, then $U_{2n} = 0$ and $U_{2n+1} = (-Q)^n$. One subsequence is constant and the other geometric. Doing without this degenerate case and, thus, assuming $P = U_2 \neq 0$ does no harm.

[†] Lucas uses the capital Greek letter Δ for the discriminant. However, for better homogeneity with the Roman letters U_n, V_n, P, and Q, we prefer the Roman letter D.

If D is zero, then the double root α is the integer $P/2$. In this case, the closed forms become

$$U_n = n\alpha^{n-1} \quad \text{and} \quad V_n = 2\alpha^n. \tag{2.6}$$

Note that one may obtain (2.6) using the Binet form (2.5) for U_n and V_n. Indeed, U_n is a symmetric polynomial in α and β since

$$U_n = \sum_{k=0}^{n-1} \alpha^{n-1-k}\beta^k,$$

so that taking the limits $\lim_{\beta\to\alpha} U_n$ and $\lim_{\beta\to\alpha} V_n$ in (2.5) yields (2.6).

Whenever $D \neq 0$, we refer to U (and V) as being *nonzero-discriminant* or *standard* Lucas sequences. Thus, nonstandard Lucas sequences satisfy (2.6), whereas standard ones satisfy (2.5).

Example 1 The pairs $\{(I_n), 2\}$, $\{(M_n), (2^n + 1)\}$, and $\{(F_n), (L_n)\}$ are particular $\{U, V\}$ pairs. Here, $I_n := n$ is the identity sequence, $M_n := 2^n - 1$ is the sequence of Mersenne numbers, and F denotes the Fibonacci sequence and L the sequence of Lucas numbers. The three corresponding values of (P, Q) are, respectively, $(2, 1)$, $(3, 2)$, and $(1, -1)$. The numbers $\frac{q^n-1}{q-1}$, which appear in Gaussian or q-binomial coefficients, if one sets the parameter q to be a fixed integer, form the Lucas sequences $U(q + 1, q)$.[†] □

2.2 Most Common Identities

Because of the correspondence with trigonometry, identities are plentiful. The purpose of this section is only to present those identities which appear in many contexts. They are the most important. These include the Pythagorean, the double-angle, the addition, the subtraction, and several multiplication formulas. The latter three give X_{m+n}, X_{m-n}, and X_{mn} in terms of X_m, X_m^*, X_n, and X_n^*, where $\{X, X^*\} = \{U, V\}$. All the formulas shown in this section except for the identity (2.42) can be found in Lucas' work, and we occasionally point out exactly where.

The two Binet forms (2.5) and (2.6) permit us to extend the definition of Lucas sequences to negative indices.[‡]

Thus, we obtain formulas that correspond to $\sin(-x) = -\sin x$ and $\cos(-x) = \cos x$, namely, for all integers n

[†] Nowhere in Lucas' writings is there a hint of his being aware of Gaussian coefficients even though one could have fancied his use of the letters P and Q came from there.

[‡] Doing so corresponds to running the recursion (2.1) backward. Indeed, $(x - \alpha^{-1})(x - \beta^{-1}) = x^2 - Q^{-1}Px + Q^{-1}$. But $U_{-(n+2)} = Q^{-1}PU_{-(n+1)} - Q^{-1}U_{-n}$ is equivalent to $U_{-n} = PU_{-n-1} - QU_{-n-2}$.

$$Q^n U_{-n} = -U_n \quad \text{and} \quad Q^n V_{-n} = V_n. \tag{2.7}$$

The former formula in (2.7) is seen to hold because, if $D \neq 0$, then

$$\delta Q^n U_{-n} = (\alpha\beta)^n(\alpha^{-n} - \beta^{-n}) = \beta^n - \alpha^n = -\delta U_n,$$

while, if $D = 0$, then

$$Q^n U_{-n} = \alpha^{2n} \cdot (-n)\alpha^{-n-1} = -n\alpha^{n-1} = -U_n.$$

Similarly,

$$Q^n V_{-n} = (\alpha\beta)^n(\alpha^{-n} + \beta^{-n}) = \beta^n + \alpha^n = V_n.$$

The *Pythagorean* formula $\cos^2 x + \sin^2 x = 1$ is embedded in the form

$$V_n^2 - DU_n^2 = 4Q^n. \tag{2.8}$$

From $\delta U_n = \alpha^n - \beta^n$ and $V_n = \alpha^n + \beta^n$, we obtain the two identities

$$\begin{aligned} V_n + \delta U_n &= 2\alpha^n, \\ V_n - \delta U_n &= 2\beta^n, \end{aligned} \tag{2.9}$$

which when multiplied together yield (2.8). If $\alpha = \beta$, i.e., if $\delta = 0$, then (2.8) is readily seen to hold.

In correspondence with the trigonometric identities

$$\begin{aligned} \sin(x + y) &= \sin x \cos y + \sin y \cos x, \\ \cos(x + y) &= \cos x \cos y - \sin x \sin y, \end{aligned}$$

we have the so-called *addition* formulas of Lucas [12, Sect. IX]

$$2U_{m+n} = U_m V_n + U_n V_m, \tag{2.10}$$

$$2V_{m+n} = V_m V_n + DU_m U_n. \tag{2.11}$$

The *subtraction* formulas are

$$2Q^n U_{m-n} = U_m V_n - U_n V_m, \tag{2.12}$$

$$2Q^n V_{m-n} = V_m V_n - DU_m U_n. \tag{2.13}$$

To prove these or other identities, we may use the Binet formulas for U_n and V_n, but another method which we will refer to as the RIC method (RIC standing for "recursion plus initial conditions") is often handy. If there are several variables as in (2.10) where we have the two variables m and n, we fix one of the variables to an arbitrary value. Then we compare the recursions satisfied by both the left and the right sides of the equation. If those recursions agree and have order r, then we compare initial conditions or the coincidence of any r consecutive values. For instance, for (2.10), say

we fix m. Then the functions $n \mapsto 2U_{m+n}$ and $n \mapsto U_m \cdot V_n + V_m \cdot U_n$ both satisfy the second-order recursion (2.1). We compare initial conditions, say at $n = 0$ and $n = 1$. For $n = 0$, both sides are equal to $2U_m$. Replacing n by 1 in (2.10), we obtain $2U_{m+1} = PU_m + V_m$. But this identity itself is easily checked by RIC. Both sides are functions of m that satisfy the same order-two recursion and take the values 2 and $2P$ for the respective values 0 and 1 of m. This proves the summation formula for fundamental Lucas sequences. The RIC technique works just as well for identity (2.11).

The subtraction formulas are a direct consequence of the addition formulas. For instance, using (2.10) and (2.7), we find that

$$\begin{aligned} 2Q^n U_{m-n} &= 2Q^n U_{m+(-n)} = Q^n(U_m V_{-n} + U_{-n} V_m) \\ &= U_m(Q^n V_{-n}) + (Q^n U_{-n}) V_m = U_m V_n - U_n V_m. \end{aligned}$$

Remark 3 At this point, we wish to clarify the extent to which all formulas in this section are valid. They hold for all Lucas sequences including degenerate, zero-discriminant, or nonregular cases. Moreover, most are valid for all integral indices, not just nonnegative indices, unless otherwise stated. Also, the limit argument by which we obtained the Binet forms (2.6) from (2.5) may seem somewhat dubious: On what β-support do we take the limit as $\beta \to \alpha$? Besides, α is often not a fixed target as β changes. But the argument can be made rigorous. Indeed, a formula involving U and/or V terms at a few indices as well as possibly P, Q, and D can be transformed into a two-variable expression in α and β equal to 0. Once the formula is proved for $D \neq 0$, then we may consider the polynomial in two variables that results from putting $x = \alpha$ and $y = \beta$. Occasionally, it may not be a polynomial, but by a small manipulation, it can be made to be a polynomial, e.g., if $n < 0$ in (2.12), then multiply out by Q^{-n}. Thus, we have a polynomial equal to 0 for infinitely many values of x and y. Therefore, it is zero for all values of x and y, and, in particular, the identity holds for $x = y$. Although checking out the formulas in the $D = 0$ case is often easier than the $D \neq 0$ case and may be fun to perform, it is not necessary.

Subtracting side to side (2.12) from (2.10) yields

$$U_{m+n} = V_m U_n + Q^n U_{m-n}, \tag{2.14}$$

whereas the subtraction of (2.13) from (2.11) gives

$$V_{m+n} = DU_m U_n + Q^n V_{m-n}. \tag{2.15}$$

Also adding side to side (2.12) and (2.10) yields

$$U_{m+n} = U_m V_n - Q^n U_{m-n}. \tag{2.16}$$

Similarly, the addition of (2.13) and (2.11) gives

$$V_{m+n} = V_m V_n - Q^n V_{m-n}. \tag{2.17}$$

On interchanging n with m in, respectively, (2.16) and (2.17), we obtain for either $X = U$ or $X = V$

$$X_{n+m} = V_m X_n - Q^m X_{n-m}. \tag{2.18}$$

In particular, replacing n by $m(n+1)$ in (2.18) yields

$$X_{m(n+2)} = V_m X_{m(n+1)} - Q^m X_{mn}. \tag{2.19}$$

When $m = 1$, we recover the basic defining recursion of the Lucas pair (U, V). But it also says, given any $m \geq 2$ and provided $U_m \neq 0$, that the sequences $U'_n = U_{mn}/U_m$ and $V'_n = V_{mn}$ form a derived pair of Lucas sequences associated with the parameters $P' = V_m$ and $Q' = Q^m$. Their characteristic polynomial $x^2 - V_m x + Q^m$ has zeros α^m and β^m.

In particular, we obtain the useful identities

$$U_{mn}(P, Q) = U_m(P, Q) \cdot U_n(V_m, Q^m), \tag{2.20}$$

and

$$V_{mn}(P, Q) = V_n(V_m, Q^m). \tag{2.21}$$

Remark 4 We observe that the two identities (2.20) and (2.21) are straightforward to see. Assume $\alpha^m \neq \beta^m$. Then

$$U_{mn}(P, Q) = \frac{\alpha^{mn} - \beta^{mn}}{\alpha - \beta} = \frac{\alpha^m - \beta^m}{\alpha - \beta} \cdot \frac{(\alpha^m)^n - (\beta^m)^n}{\alpha^m - \beta^m}, \tag{2.22}$$

whereas

$$V_{mn}(P, Q) = (\alpha^m)^n + (\beta^m)^n = V_n(V_m, Q^m).$$

Putting $m = n$ in (2.14), or in (2.10), we obtain the so-called *double-angle* identity

$$U_{2n} = U_n V_n. \tag{2.23}$$

By the Binet formula for V and the Pythagorean identity, we readily find identities that correspond to $\cos(2x) = 2\cos^2 x - 1 = 1 - 2\sin^2 x$, namely,

$$V_{2n} = V_n^2 - 2Q^n = DU_n^2 + 2Q^n. \tag{2.24}$$

Adding $V_n^2 - 2Q^n$ to $DU_n^2 + 2Q^n$ yields

$$2V_{2n} = V_n^2 + DU_n^2, \tag{2.25}$$

standing for $\cos(2x) = \cos^2 x - \sin^2 x$.

Replacing m by n and n by 1 in both (2.14) and (2.15) yields

$$U_{n+1} - QU_{n-1} = V_n \quad \text{and} \quad V_{n+1} - QV_{n-1} = DU_n. \tag{2.26}$$

The famous Cassini[†] identity $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$ for the Fibonacci numbers has a more general form for U sequences, and an analogous identity exists for sequences V. These are

$$U_n^2 - U_{n-1}U_{n+1} = Q^{n-1} \quad \text{and} \quad V_n^2 - V_{n-1}V_{n+1} = -DQ^{n-1}. \tag{2.27}$$

They can be proved by various techniques, e.g., using the Binet formulas, or an inductive reasoning, or matrices. For instance, if $D \neq 0$, we see that

$$\begin{aligned} D(U_n^2 - U_{n-1}U_{n+1}) &= (\alpha^n - \beta^n)^2 - (\alpha^{n-1} - \beta^{n-1})(\alpha^{n+1} - \beta^{n+1}) \\ &= -2Q^n + (\alpha^2 + \beta^2)Q^{n-1} \\ &= -2Q^n + (P^2 - 2Q)Q^{n-1} = DQ^{n-1}, \end{aligned}$$

which yields the first identity on cancelling out D.

Because, as can be verified by induction, one has for all integers n

$$\begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} U_{n+1} & -QU_n \\ U_n & -QU_{n-1} \end{pmatrix},$$

we may equate the determinants on both sides and see that

$$Q^n = -Q(U_{n+1}U_{n-1} - U_n^2),$$

yielding again the first identity in (2.27).

We now give one pair of *multiplication* formulas of Lucas [13, Sect. 183, p. 319] valid for all integers $m \geq 0$ and all integers n

$$2^{m-1}U_{mn} = \sum_{k=0}^{\lfloor (m-1)/2 \rfloor} \binom{m}{2k+1} D^k U_n^{2k+1} V_n^{m-2k-1}, \tag{2.28}$$

and

$$2^{m-1}V_{mn} = \sum_{k=0}^{\lfloor m/2 \rfloor} \binom{m}{2k} D^k U_n^{2k} V_n^{m-2k}. \tag{2.29}$$

The two identities (2.28) and (2.29) are usually proved by either subtracting or adding the two sides of (2.9) raised to the mth power. Thus, for instance, with a subtraction, we obtain

[†] The Fibonacci numbers were known to a number of early investigators, but not under that name. They were often discussed as being components of the convergents to the continued fraction expansion of the golden ratio: $(1 + \sqrt{5})/2$.

$$\begin{aligned}(2\alpha^n)^m - (2\beta^n)^m &= (V_n + \delta U_n)^m - (V_n - \delta U_n)^m \\ &= \sum_{k=0}^{m} \binom{m}{k} V_n^{m-k} (\delta U_n)^k - \sum_{k=0}^{m} \binom{m}{k} V_n^{m-k} (-\delta U_n)^k \\ &= 2 \sum_{k\geq 0} \binom{m}{2k+1} V_n^{m-2k-1} \delta D^k U_n^{2k+1},\end{aligned}$$

which after division by 2δ, assuming $D \neq 0$, yields the multiplication formula (2.28).

Lucas [13, Sect. 179, p. 312] had observed that U_n is a homogeneous polynomial of degree $n-1$ in P and Q, while V_n is a homogeneous polynomial of degree n in P and Q, provided in both cases the degree in Q is counted with double weight. That is, U_n and V_n are homogeneous polynomials in P and $\sqrt{Q}$ of respective degrees $n-1$ and n, where powers of $\sqrt{Q}$ are always even. We provide these polynomials in P and Q for $1 \leq n \leq 6$ in Table 2.1.

Table 2.1 U_n and V_n as polynomials in P and Q

n	U_n	V_n
1	1	P
2	P	$P^2 - 2Q$
3	$P^2 - Q$	$P^3 - 3PQ$
4	$P^3 - 2PQ$	$P^4 - 4P^2Q + 2Q^2$
5	$P^4 - 3P^2Q + Q^2$	$P^5 - 5P^3Q + 5PQ^2$
6	$P^5 - 4P^3Q + 3PQ^2$	$P^6 - 6P^4Q + 9P^2Q^2 - 2Q^3$

In general, we find for all $n \geq 0$

$$U_n = \Psi_n(P, Q), \tag{2.30}$$

where

$$\Psi_n = \Psi_n(P, Q) := \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} (-1)^k \binom{n-k-1}{k} P^{n-2k-1} Q^k. \tag{2.31}$$

Actually, if (X_n) satisfies the recursion (2.1), then it follows from the identity $\Psi_{n+2} = P\Psi_{n+1} - Q\Psi_n$ and induction on n that for all $n \geq 1$,

$$X_n = \Psi_n X_1 - Q\Psi_{n-1} X_0, \tag{2.32}$$

where we adopted the convention $\Psi_0 = U_0 = 0$.

Hence, $V_n = P\Psi_n - 2Q\Psi_{n-1}$, which, using

$$\binom{n-1-k}{k} + 2\binom{n-1-k}{k-1} = \frac{n}{n-k}\binom{n-k}{k}, \tag{2.33}$$

yields V_n, for all $n \geq 1$, as the homogeneous polynomials in P and $\sqrt{Q}$ on the right-hand column of Table 2.1, i.e.,

$$V_n = \sum_{k \leq \frac{n}{2}} \frac{n}{n-k} \binom{n-k}{k} P^{n-2k} (-Q)^k. \tag{2.34}$$

The multiplication formulas (2.28) and (2.29) have the peculiarity of bearing a power of 2 in front of U_{mn} and V_{mn}. But Lucas [12, Sects. XII–XIII], [13, Sect. 183, p. 318] also considered another set of *multiplication* formulas expressing U_{mn}/U_n and V_{mn} as polynomials in V_n and Q. These formulas extend the double-angle formula (2.23). They correspond to the de Moivre formulas giving $\frac{\sin(mx)}{\sin x}$ and $\cos(mx)$ as polynomials in $\cos x$, as Lucas himself pointed out [12, Sects. XII, p. 208]. Thus, for $m \geq 1$ and $n \geq 1$, we have

$$U_{mn} = U_m \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} \binom{n-k-1}{k} (-1)^k \, Q^{km} V_m^{n-2k-1}, \tag{2.35}$$

and

$$V_{mn} = \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{n}{n-k} \binom{n-k}{k} (-1)^k \, Q^{km} V_m^{n-2k}. \tag{2.36}$$

To derive (2.35), one can use the identities (2.30) and (2.31) with $P = V_m$ and $Q = Q^m$. Hence,

$$\Psi_n(V_m, Q^m) = \sum_{k < \frac{n}{2}} (-1)^k \binom{n-1-k}{k} V_m^{n-1-2k} Q^{mk} = U_{mn}/U_m.$$

We note that (2.34) can also be viewed as a particular instance of the formal polynomial identity in A and B:

$$A^n + B^n = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \frac{n}{n-k} \binom{n-k}{k} (AB)^k (A+B)^{n-2k}. \tag{2.37}$$

(Identity (2.37) can also easily be derived by appealing to an instance of the Girard-Waring formula—see, for example, [6].) Lucas used (2.37) to produce yet another pair of multiplication formulas. Replacing n by m in (2.37), and then putting $A = \alpha^n$ and $B = -\beta^n$, we get for odd m

$$U_{mn} = \sum_{k=0}^{(m-1)/2} \frac{m}{m-k} \binom{m-k}{k} Q^{kn} D^{(m-2k-1)/2} U_n^{m-2k} \tag{2.38}$$

and for even m

$$V_{mn} = \sum_{k=0}^{m/2} \frac{m}{m-k} \binom{m-k}{k} Q^{kn} D^{(m-2k)/2} U_n^{m-2k}. \tag{2.39}$$

Also, $2^{n-1}U_n$ and $2^{n-1}V_n$ can be expressed as homogeneous polynomials in P and D, if degrees in D are doubled. Indeed,

$$2^{n-1}U_n = \sum_{k\geq 0} \binom{n}{2k+1} P^{n-2k-1} D^k, \tag{2.40}$$

and

$$2^{n-1}V_n = \sum_{k\geq 0} \binom{n}{2k} P^{n-2k} D^k. \tag{2.41}$$

As Lucas did [13, p. 317], this can be proved by expanding the binomial formula (2.4) on α and β, i.e.,

$$\begin{aligned} 2^n \delta U_n &= 2^n(\alpha^n - \beta^n) = (P+\delta)^n - (P-\delta)^n \\ &= \sum_k \binom{n}{k} P^{n-k}\delta^k - \sum_k \binom{n}{k} P^{n-k}(-\delta)^k \\ &= 2\sum_{k \text{ odd}} \binom{n}{k} P^{n-k}\delta^k = 2\delta \sum_{k\geq 0} \binom{n}{2k+1} P^{n-2k-1} D^k, \end{aligned}$$

which upon division by 2δ yields (2.40). Formula (2.41) can be obtained by expanding similarly $2^n V_n = (P+\delta)^n + (P-\delta)^n$.

Another useful identity, valid for all integers m and n, is given below

$$U_m = U_{n+1}U_{m-n} - QU_nU_{m-n-1}. \tag{2.42}$$

The RIC method works well. (Fix m to an arbitrary integer value. Then check the identity for the two consecutive values m and $m+1$ of n using (2.7).) We observe that (2.42) is also often used in the equivalent form

$$U_{m+n} = U_mU_{n+1} - QU_{m-1}U_n. \tag{2.43}$$

Putting $m = n+1$ in (2.43) yields the identity

$$U_{2n+1} = U_{n+1}^2 - QU_n^2, \tag{2.44}$$

which for the Fibonacci sequence $F = U(1,-1)$ gives the classical formula

$$F_{2n+1} = F_n^2 + F_{n+1}^2. \tag{2.45}$$

Not to prejudice the V-side of Lucas sequences, we provide an identity somewhat like (2.42), but for companion sequences, namely,

$$V_m = U_{n+1}V_{m-n} - QU_nV_{m-n-1}. \tag{2.46}$$

2.3 General Divisibility Properties

Although the Lucas sequences are second-order linear recurrences and as such are defined additively, they, perhaps surprisingly, possess divisibility properties. In fact, these multiplicative properties form an important key feature of these sequences.

A sequence of integers $(X_n)_{n\geq 0}$, satisfying $X_0 = 0$ and

$$m \mid n \implies X_m \mid X_n, \tag{2.47}$$

for all $0 < m < n$ is said to be a *divisibility sequence*, or less frequently a *divisible sequence*. Note, in particular, that if $X_m = 0$, then $X_n = 0$ for all multiples n of m.

We assume the integers m and n to be nonnegative throughout this section.

Lemma 1 *The parity of U_n and V_n, $n \geq 0$, is given by the rules:*

$$\begin{aligned} Q \text{ even and } P \text{ odd} &\implies \text{all } X_n,\ n \geq 1, \text{ are odd.} \\ Q \text{ and } P \text{ even} &\implies \text{all } X_n,\ n \geq 0, \text{ are even, except for } U_1. \\ PQ \text{ odd} &\implies 2 \mid X_n \iff 3 \mid n. \\ Q \text{ odd and } P \text{ even} &\implies 2 \mid V_n, \text{ for all } n \geq 0, \text{ and } 2 \mid U_n \iff 2 \mid n, \end{aligned}$$

where X stands for U or V.

Proof These implications are readily seen by applying the recursion (2.1) modulo 2. For instance, for the last two where Q is odd, we find that if P is odd, then both U and $V \pmod 2$ are

$$0, 1, 1, 0, 1, 1, \ldots, 0, 1, 1, \ldots$$

In particular, $2 \mid X_n \iff 3 \mid n$, where X is either U or V. If P is even, then all V terms are even, while only even-indexed U terms are even. □

Theorem 2 *The sequence $U = U(P, Q)$ is a divisibility sequence, i.e.,*

$$m \mid n \implies U_m \mid U_n.$$

Proof This is a direct consequence of identity (2.20) or of formula (2.35). □

Remark 5 An alternate proof of Theorem 2 may be obtained from the multiplication formula (2.28). Say $n = km$. Then applying the formula to U_{km}, we see that U_m divides $2^{k-1}U_n$. Thus, if U_m is odd, then the theorem follows. If U_m is even, then, by Lemma 1, V_m is also even. Hence, each term of the sum $\sum_{i=0}^{\lfloor (k-1)/2 \rfloor} \binom{k}{2i+1} D^i U_m^{2i+1} V_m^{k-2i-1}$ is individually divisible by $2^{k-1}U_m$.

If $a \geq 2$ is an integer, then it has been known at least since the time of Fermat that

$$\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1. \tag{2.48}$$

Indeed, without loss of generality, we may suppose $m \geq n > 0$. Say $m = qn+r$ with $0 \leq r < n$. To show (2.48) holds, it suffices to check that

$$\gcd(a^m - 1, a^n - 1) = \gcd(a^n - 1, a^r - 1).$$

From the identity

$$a^m - 1 = a^{qn+r} - 1 = a^r(a^n)^q - a^r + a^r - 1 = a^r\left((a^n)^q - 1\right) + a^r - 1,$$

we see that any common factor of $a^m - 1$ and $a^n - 1$ is also a common factor of $a^n - 1$ and $a^r - 1$ and vice versa.

After dividing equation (2.48) through by $a-1$, we obtain that $U(a+1, a)$ is a *strong divisibility* sequence, i.e., a sequence of integers $(X_t)_{t\geq 0}$ such that for all $m \geq n > 0$, we have

$$\gcd(X_m, X_n) = |X_{\gcd(m,n)}|. \tag{2.49}$$

The next theorem pins down a necessary and sufficient condition on P and Q which makes $U(P, Q)$ strongly divisible.

Theorem 3 *For all $m \geq n > 0$, the sequence $U(P, Q)$ satisfies*

$$\gcd(U_m, U_n) = |U_{\gcd(m,n)}| \text{ if and only if } \gcd(P, Q) = 1.$$

A Lucas sequence $U(P, Q)$ with $\gcd(P, Q) = 1$ is called *regular*.

Before proving Theorem 3, we establish a few useful lemmas.

Lemma 2 *If U is regular, then*

$$\gcd(U_n, Q) = \gcd(V_n, Q) = 1,$$

for all $n \geq 1$.

Proof Let X be U or V. By (2.1), we see that $X_{n+2} \equiv PX_{n+1} \pmod{Q}$, $(n \geq 0)$. As $U_1 = 1$ and $V_1 = P$, a simple induction shows that $U_n \equiv P^{n-1} \pmod{Q}$ and $V_n \equiv P^n \pmod{Q}$ for all $n \geq 1$. Thus, if a prime p divides both X_n and Q, then $p \mid P^n$. Thus, $p \mid \gcd(P, Q)$. This contradicts the hypothesis. □

Lemma 3 *Let U, V be a pair of Lucas sequences. Then for all $n \geq 0$,*

$$\gcd(U_n, V_n) \mid 2Q^{\lfloor n/2 \rfloor}.$$

Proof The lemma is a direct consequence of the Pythagorean identity (2.8)

$$V_n^2 - DU_n^2 = 4Q^n.$$

Lemma 4 *If U is regular, then for all $n \geq 1$,*

$$\gcd(U_n, V_n) = 1 \text{ or } 2$$

and $\gcd(U_n, V_n) = 1$*, if, in addition, Q is even.*

Proof By Lemma 2, no factor $d > 1$ of Q may divide U_n. Hence, we see the result holds by Lemma 3. □

First proof of Theorem 3. If $\gcd(P, Q) > 1$, then $\gcd(P, P^2 - Q) = \gcd(U_2, U_3) > 1$, while $U_{\gcd(2,3)} = U_1 = 1$. Thus, regularity is necessary for U to be strongly divisible.

We now show regularity is sufficient, and thus, we assume $\gcd(P, Q) = 1$. By Theorem 2, $U_{\gcd(m,n)} \mid \gcd(U_m, U_n)$. Thus, assuming as we did prior to the theorem, that $m = qn + r$, $0 \leq r < n$, by the Euclidean algorithm, all we need to show is that $G := \gcd(U_m, U_n)$ divides U_r. Since $m - r = qn$, we obtain by the subtraction formula (2.12) that

$$V_r U_m - 2Q^r U_{qn} = V_m U_r. \tag{2.50}$$

Since $G \mid U_m$ and, by Theorem 2, $G \mid U_{qn}$, we find that $G \mid V_m U_r$. If $\gcd(U_m, V_m) = 1$, then G is prime to V_m so G divides U_r. Thus, by Lemma 4, we may now assume Q odd and $\gcd(U_m, V_m) = 2$. Let us write $G = 2^\nu g$ with g odd. As g is prime to V_m, $g \mid U_r$. Thus, it remains to see that $2^\nu \mid U_r$, assuming $\nu \geq 1$.

We use Lemma 1 when Q is odd. If P is odd, then as both U_m and U_n are even, m and n are multiples of 3. Thus, $3 \mid r$. Hence, $2 \mid U_r$. If P is even, then the evenness of U_m and U_n means that m and n are even. Thus, r is even and again $2 \mid U_r$. There is nothing more to prove if $\nu = 1$. Hence, suppose $\nu \geq 2$. Then $4 \mid U_m$. So $2 \,||\, V_m$. But whatever the parity of P, $2 \mid U_r$ implies V_r is even. Hence, $2^{\nu+1}$ divides the left-hand side of (2.50) and so $2^\nu \mid U_r$.

However, a simpler proof of the core part of Theorem 3, i.e., of the fact that P and Q are coprime implies $\gcd(U_m, U_n) = \pm U_{\gcd(m,n)}$, is often achieved using identity (2.42). But we need another preliminary lemma.

Lemma 5 *If* $\gcd(P, Q) = 1$*, then* $\gcd(U_n, U_{n+1}) = 1$ *for all* $n \geq 0$.

Proof We proceed by induction. Indeed, $\gcd(U_0, U_1) = 1$. Say $\gcd(U_n, U_{n+1}) = 1$ for some $n \geq 0$. If $\gcd(U_{n+1}, U_{n+2}) > 1$, then some prime p divides U_{n+1} and $U_{n+2} = PU_{n+1} - QU_n$. Thus, $p \mid QU_n$. But by Lemma 2, $p \mid U_{n+1}$ implies $p \nmid Q$. Hence, $p \mid U_n$, which contradicts $\gcd(U_n, U_{n+1}) = 1$. □

Second proof of Theorem 3. To prove that $\gcd(U_m, U_n) = \pm U_{\gcd(m,n)}$, it suffices to show that $\gcd(U_m, U_n) = \gcd(U_{m-n}, U_n)$. But by (2.42),

$$\begin{aligned} \gcd(U_m, U_n) &= \gcd(U_{n+1}U_{m-n} - QU_nU_{m-n-1}, U_n) \\ &= \gcd(U_{n+1}U_{m-n}, U_n) = \gcd(U_{m-n}, U_n), \end{aligned}$$

where the last step follows from Lemma 5.

Companion sequences are not divisibility sequences. Nevertheless, they satisfy a weaker divisibility condition given in Theorem 4. This theorem generalizes the well-known fact that for a and b integers and m odd, we have

$$a^n + b^n \text{ divides } a^{mn} + b^{mn}.$$

Theorem 4 *Let V be a companion Lucas sequence. Then*

$$m \text{ odd} \implies V_n \mid V_{mn}.$$

Proof By (2.33), all terms of the sum appearing on the right-hand side of (2.36) are integers. Hence, for m odd, we see that V_n divides V_{mn}. □

Second proof of Theorem 4. We can also wrestle out a proof from the multiplication formula (2.29). Indeed, (2.29) tells us that V_n divides $2^{m-1}V_{mn}$. If V_n is odd, then $V_n \mid V_{mn}$. If V_n is even, then either P is even, or both P and Q are odd by Lemma 1. If P is even, then $4 \mid D$ so that each term of the sum (2.29) being a multiple of $D^k V_n^{m-2k-1} V_n$ is a multiple of $4^k 2^{m-2k-1} V_n = 2^{m-1} V_n$. If PQ is odd, then, by Lemma 1, $3 \mid n$ and $2 \mid U_n$. But each term of the right-hand side sum of (2.29) contains the factor $U_n^{2k} V_n^{m-2k-1} V_n$ which is divisible by $2^{m-1}V_n$.

Third proof of Theorem 4. Using congruences in the ring of integers $\mathcal{O}$ of the root field $\mathbb{Q}(\alpha)$ and bearing in mind that $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$, the proof is simple. Indeed, $V_n = \alpha^n + \beta^n \implies \alpha^n \equiv -\beta^n \pmod{V_n}$. Raising the congruence to the odd mth power, we obtain $\alpha^{mn} \equiv -\beta^{mn} \pmod{V_n}$. That is, $V_n \mid V_{mn}$.

Fourth proof of Theorem 4. By Galois theory, any symmetric polynomial expression in the algebraic integers $x = \alpha^n$ and $y = \beta^n$ must be a rational integer. Now

$$\begin{aligned} V_{mn} &= x^m + y^m = x^m - (-y)^m \\ &= \big(x - (-y)\big) \sum_{i=0}^{m-1} x^{m-1-i}(-y)^i = V_n \sum_{i=0}^{m-1} (-1)^i x^{m-1-i} y^i. \end{aligned}$$

Since $(-1)^i = (-1)^{m-1-i}$, the sum $\sum_{i=0}^{m-1} (-1)^i x^{m-1-i} y^i$ is a symmetric polynomial in x and y. Thus, $V_n \mid V_{mn}$.

There is also a weaker form of Theorem 3 which applies to companion sequences when we consider indices m and n that belong to the same 2-adic class, i.e., that have the same 2-adic valuation.

Theorem 5 *Let* $\gcd(P, Q) = 1$, $m \geq n \geq 1$. *Then*

$$m \sim_2 n \implies \gcd(V_m, V_n) = |V_{\gcd(m,n)}|.$$

We postpone the proof of Theorem 5 till Sect. 2.9, where it is a direct consequence of Corollary 30 and of the fact that no regular prime dividing Q may divide any V term.

It is often useful to be aware that Theorem 3 remains nearly true when $\gcd(P,Q) > 0$. A prime p is said to be *regular* if and only if $p \nmid \gcd(P,Q)$. A prime that divides $\gcd(P,Q)$ is called *special*.

Lemma 6 *Suppose p is a regular prime. Then either $p \nmid Q$, or $p \mid Q$ and does not divide any U_n, $n \geq 1$.*

Proof If $p \mid Q$, then $p \nmid P$ since p is regular. Therefore, as seen in Lemma 2, $U_n \equiv P^{n-1} \pmod{p}$. The conclusion follows. □

Lemma 7 *If $p \nmid Q$, then $\gcd(U_n, U_{n+1})$ is prime to p for all $n \geq 1$.*

Proof This follows by induction for $p \nmid U_1$ and if $p \nmid \gcd(U_n, U_{n+1})$, then $p \nmid \gcd(U_{n+1}, U_{n+2})$. Indeed, if $p \mid U_{n+1}$ and $p \mid U_{n+2}$, then $p \mid PU_{n+1} - QU_n$, which implies $p \mid U_n$ and leads to a contradiction. □

Theorem 6 *Let $U(P,Q)$ be a fundamental Lucas sequence and p be a regular prime. Then for all $m \geq n > 0$, we have*

$$\gcd(U_m, U_n) \sim U_{\gcd(m,n)} \quad (\textit{base } p). \tag{2.51}$$

Proof Suppose $p \mid Q$. Then no U_n, $n > 0$, is divisible by p by Lemma 6. Hence, (2.51) holds. Thus, assume $p \nmid Q$. Because $U_{\gcd(m,n)}$ divides U_m and U_n, we find that $\nu_p(U_{\gcd(m,n)}) \leq \nu_p(\gcd(U_m, U_n))$. So it suffices to see that $p^\alpha \mid \gcd(U_m, U_n)$ implies $p^\alpha \mid U_{m-n}$. As in our second proof of Theorem 3, we use identity (2.42) by which $p^\alpha \mid U_{n+1}U_{m-n}$. By Lemma 7, $p \nmid U_{n+1}$. Thus, $p^\alpha \mid U_{m-n}$. □

Corollary 7 If $\ell \geq 2$ is an integer prime to Q, then for all $m \geq n > 0$,

$$\ell \mid \gcd(U_m, U_n) \iff \ell \mid U_{\gcd(m,n)}.$$

Proof By the hypothesis, all prime divisors of ℓ are regular. So by Theorem 6, if $p \mid \ell$, then the p-adic valuations of $\gcd(U_m, U_n)$ and of $U_{\gcd(m,n)}$ are identical. Thus, the corollary must hold. □

Definition 1 (Rank of appearance) Let $m \geq 2$ be an integer. We define the rank, or the rank of appearance of m in U, denoted as $\rho = \rho_U(m)$, to be the least positive index t such that $m \mid U_t$, whenever such an integer ρ exists.[†]

[†] Lucas used the letter ω for the rank, maybe, or maybe not, in connection with the period of elliptic functions. We prefer ρ, the Greek r, for rank and reserve the Roman r for a variable name.

Lucas called it in French *le rang d'apparition de* m, and the French word "apparition" has been—and still is—widely in use among English writers. However, in English, more so than in French, the word "apparition" has a ghostly or miraculous connotation which is best to avoid: There is nothing supernatural about how integers divide terms of Lucas sequences. The rank ρ is sometimes called the *entry point* of m in U. In this case, the letter z often denotes the entry point.

Lemma 8 *If $m \geq 2$ is an integer coprime to Q, then the rank $\rho(m)$ exists.*

Proof We need to show the existence of a positive integer t such that $U_t \equiv 0 \pmod{m}$. The sequence $(U_n \pmod{m})$ may only take at most m^2 distinct pairs of consecutive values. Therefore, from some point on, it must repeat itself going forward and be periodic since $U \pmod{m}$ is determined by two consecutive values of $(U_n \pmod{m})$. However, because $\gcd(Q, m) = 1$, the inverse of $Q \pmod{m}$ is well defined, and the recurrence $(U_n \pmod{m})$ may be run backward as well as forward. Indeed, $U_{-(n+2)} = Q^{-1}PU_{-(n+1)} - Q^{-1}U_{-n}$. Thus, it is fully periodic over $\mathbb{Z}$. Since $U_0 = 0$, the value $0 \pmod{m}$ must repeat itself in both directions. In particular, there is a minimal $t > 0$ for which $m \mid U_t$. □

We now establish an important theorem concerning $\rho(m)$. This theorem does not bear a traditional name, but we refer to it as the *law of regular division* since it says that a regular divisor m divides the terms of the sequence U precisely every ρ term.

Theorem 8 *If $m \geq 2$ is prime to Q of rank ρ, then*

$$m \mid U_n \iff \rho \mid n.$$

Proof Clearly, $m \mid U_n$ if and only if $m \mid \gcd(U_n, U_\rho)$. By Corollary 7, this occurs if and only if $m \mid U_{\gcd(n,\rho)}$. By the definition of ρ, $m \mid U_{\gcd(n,\rho)}$ is true if and only if $\rho = \gcd(n, \rho)$, i.e., if and only if $\rho \mid n$. □

2.4 Divisibility of U_n by Powers of an Odd Prime

From Lemma 8, if $p \nmid Q$ is a prime, then we know all powers p^a, $a \geq 1$, do divide some terms of $U(P, Q)$. Moreover, we know which terms are divisible by a given prime power p^a once we know its rank by Theorem 8. In this section, we gather more information on the values of the ranks of primes and see precisely how the rank of a prime power p^{a+1} relates to the rank $\rho(p^a)$ of the previous power p^a.

If p is special, then p divides all U_n, $n \geq 2$. If $p \mid Q$, but $p \nmid P$, then no U_n, $n \geq 1$, is divisible by p by Lemma 6. To express the *law of appearance* for primes not dividing Q, we use the symbol ϵ_p to denote the Legendre character $(D \mid p)$. That is,

$$\epsilon_p = (D \,|\, p) = \begin{cases} 0, & \text{if } p \mid D; \\ 1, & \text{if } D \text{ is a nonzero square modulo } p; \\ -1, & \text{if } D \text{ is not a square modulo } p. \end{cases} \tag{2.52}$$

We begin with a lemma.

Lemma 9 *If p is an odd prime, then*

$$U_p \equiv \epsilon_p \pmod{p} \quad \textit{and} \quad V_p \equiv P \pmod{p}.$$

Proof As the binomial coefficient $\binom{p}{2k+1}$ is divisible by p unless $k = (p-1)/2$, we obtain by setting $n = p$ in (2.40) that $2^{p-1}U_p \equiv D^{\frac{p-1}{2}} \pmod{p}$. This implies $U_p \equiv \epsilon_p \pmod{p}$. Similarly, (2.41) gives $2^{p-1}V_p \equiv \binom{p}{0}P^p \pmod{p}$, yielding $V_p \equiv P \pmod{p}$. □

Remark 6 Rather than using Equations (2.40) and (2.41), we may use congruences in the ring of integers $\mathcal{O}$ of the field $\mathbb{Q}(\alpha)$. Indeed, $V_p = \alpha^p + \beta^p \equiv (\alpha+\beta)^p = P^p \equiv P \pmod{p\mathcal{O}}$ implying $V_p \equiv P \pmod{p}$ since V_p and P are rational integers. Likewise, assuming $p \nmid D$, we find that

$$U_p \equiv \frac{(\alpha-\beta)^p}{\alpha-\beta} = (\alpha-\beta)^{p-1} = D^{\frac{p-1}{2}} \equiv \epsilon_p \pmod{p\mathcal{O}}.$$

Theorem 9 (Law of appearance for primes) *Suppose $p \nmid Q$ is a prime of rank ρ. Then we find that*

$$\textit{if } p \geq 3, \textit{ then } \rho \textit{ divides } p - \epsilon_p, \quad \textit{and}$$

$$\textit{if } p = 2, \textit{ then } \rho = \begin{cases} 2, & \textit{if } 2 \mid P; \\ 3, & \textit{if } P \textit{ is odd.} \end{cases}$$

Proof The case $p = 2$ is immediate as $U_2 = P$ and $U_3 = P^2 - Q$. Suppose p is an odd prime. We are about to see that $p \mid U_{p-\epsilon_p}$. If $\epsilon_p = 0$, then $p \mid U_p$ by Lemma 9. If $\epsilon_p = \pm 1$, then Equation (2.12) gives $2Q^{\epsilon_p}U_{p-\epsilon_p} = U_pV_{\epsilon_p} - U_{\epsilon_p}V_p$. That is, for $\epsilon_p = 1$, $2QU_{p-1} = PU_p - V_p \equiv P\epsilon_p - P = 0 \pmod{p}$, by Lemma 9. For $\epsilon_p = -1$, we get $2Q^{-1}U_{p+1} = U_pV_{-1} - U_{-1}V_p$, which when multiplied by Q yields $2U_{p+1} = U_pV_1 + V_p \equiv \epsilon_pP + P = 0 \pmod{p}$, by (2.7) and Lemma 9. Thus, by Theorem 8, we conclude that ρ divides $p - \epsilon_p$. □

Remark 7 The content of Theorem 9 can be found in [12, Sect. XXV] which Lucas titled "De l'apparition des nombres premiers ..." So Theorem 9 is Lucas' so-called law of appearance.

Remark 8 One may view the law of appearance for primes as a near generalization of Fermat's little theorem, that is, of the Fermat congruence $a^{p-1} \equiv 1 \pmod{p}$, for integers a such that $p \nmid a$. If $U = U(a+1, a)$ and $p \nmid a(a-1)$ is an odd prime, then $D = (a-1)^2$, $\epsilon_p = 1$, and the law of appearance implies

that $a^{p-1} \equiv 1 \pmod{p}$. (Since there is hardly anything to prove if $p = 2$ and a is odd, or if p is odd and $p \mid a - 1$, this law may actually be viewed as a full generalization of the Fermat congruence.)

Remark 9 The law of appearance when $\epsilon_p = -1$ may be seen via algebraic number theory. The non-trivial automorphism σ of $\mathbb{Q}(\alpha)/\mathbb{Q}$, which sends $\alpha \mapsto \beta$ and vice versa, is the Frobenius automorphism of $p\mathcal{O}/p$. That is, $\sigma(x) \equiv x^p \pmod{p\mathcal{O}}$ for all $x \in \mathcal{O}$. Thus, $Q = \alpha\beta \equiv \alpha\alpha^p \equiv \beta^p\beta \pmod{p\mathcal{O}}$. But, by (2.5), $\alpha^{p+1} \equiv \beta^{p+1} \pmod{p\mathcal{O}}$ holds iff $p \mid U_{p+1}$.

We now turn to the appearance of prime powers.

Lemma 10 *For m and n nonnegative integers, we find that*

$$2^{m-1}U_{mn} \equiv mU_nV_n^{m-1} \pmod{U_n^3}.$$

Proof This is an immediate consequence of the multiplication formula (2.28) since modulo U_n^3, only the term corresponding to $k = 0$ survives. □

We are now ready for a famous lemma which, essentially, asserts that the appearance of higher powers of p in $U_{m\rho}$ is governed by the power of p in m.

Lemma 11 (Lifting-the-exponent lemma) *Suppose $p \nmid 2Q$ is a prime that divides U_n. Then*

$$U_{mn} \sim mU_n \quad (\textit{base } p).$$

Proof We proceed by induction on ℓ where $m \sim_p p^\ell$. If $\ell = 0$ or $\ell = 1$, then we can downgrade the modulus in Lemma 10 to p^2U_n and obtain that

$$2^{m-1}U_{mn} \equiv mU_nV_n^{m-1} \pmod{p^2U_n}.$$

By Lemma 3, $p \nmid V_n^{m-1}$. Thus, $\nu_p(mU_nV_n^{m-1}) = \nu_p(mU_n) < \nu_p(p^2U_n)$ so that $U_{mn} \sim_p mU_n$. Thus, the lemma holds for $\ell \leq 1$. In particular, $U_{pn} \sim_p pU_n$ for all $n \geq 0$. Assume the lemma holds for some $\ell \geq 1$. Put $m = kp^{\ell+1}$, $p \nmid k$. Then, as $U_{pn} \sim_p pU_n$, we may use the inductive hypothesis and write that

$$U_{mn} = U_{kp^\ell(pn)} \sim kp^\ell U_{pn} \sim kp^{\ell+1}U_n = mU_n \quad (\text{base } p).$$

□

Remark 10 Lemma 11 is essentially what Lucas [12, Sect. XIII] twice called "la loi de la répétition," which translates into "the law of the repetition" (of the prime numbers). Thus, in English, for many authors who have worked with the Lucas functions, Lemma 11 is referred to as *the law of repetition*. Note that on [12, p. 210] of that same Sect. 13, Lucas also refers to this phenomenon as the "appearance of the successive powers of prime numbers."

Example 10 In the Fibonacci sequence, $\rho(3) = 4$. Thus, $3 \mid F_n$ if and only if $4 \mid n$. Moreover, $F_{4m} \sim_3 mF_4 = 3m$. For instance, $3^3 \,||\, F_{36}$. □

Remark 11 Theorem 9 and Lemma 11 provide respective proofs that a prime $p \nmid Q$ possesses a rank and that this is equally true of all its powers. These proofs are independent of the argument used in Lemma 8. Indeed, Theorem 9 shows that $p \mid U_{p-\epsilon_p}$, and the proof of Lemma 11 does not refer to Lemma 8.

Corollary 11 Suppose $p \nmid 2Q$ is a prime of rank ρ in U, and assume $p^\nu \,||\, U_\rho$. Then

$$\rho_U(p^a) = \begin{cases} \rho, & \text{if } 1 \le a \le \nu; \\ p^{a-\nu}\rho, & \text{if } a > \nu. \end{cases}$$

Proof If $1 \le a \le \nu$, then no term U_t with $0 < t < \rho$ is divisible by p. Thus, $\rho(p^a) = \rho$. If $a > \nu$, then, by Lemma 11, the least t such that p^a divides U_t is $p^{a-\nu}\rho$. □

Definition 2 (Rank exponent of a prime) Given $p \nmid Q$ of rank ρ, we define the *rank exponent* ν of p as the full exponent of p in U_ρ. That is, as in Corollary 11, $p^\nu \,||\, U_\rho$. Note that if $U_\rho = 0$, then we agree that $\nu = +\infty$.

Remark 12 Given a prime p, it is easy to construct a Lucas sequence $U(P, Q)$ such that the rank exponent ν of p is as large as we wish. A cheesy solution is to choose $P = p^\nu$. Another would be to pick P prime to p and choose $Q = P^2 - p^\nu$ so that $\rho(p) = \rho(p^\nu) = 3$. In the particular case of the Fibonacci sequence, no prime p has yet been found for which $\nu \ge 2$. There is a folk conjecture, sometimes referred to as the Wall-Sun-Sun conjecture, which asserts that $p^2 \nmid F_{\rho(p)}$ for all primes p. See [8] for an extensive bibliography on this conjecture. Although all primes $< 9.7 \times 10^{14}$ satisfy $p \,||\, F_\rho$ [4], there is little evidence from a probabilistic point of view for the truth of such a statement. The root $\alpha = \frac{1+\sqrt{5}}{2}$ is a fundamental unit of the corresponding ring of integers $\mathbb{Z}[\alpha]$ of $\mathbb{Q}(\alpha)$. We think a statistical study of rank exponents of primes in Lucas sequences built on other fundamental units would be welcome.

Remark 13 In view of the importance of Fermat's last theorem in Lucas' investigations and related to the occurrence of rank exponents larger than 1, it is interesting to note that in 1909, Arthur Wieferich showed that if p is a prime and

$$x^p + y^p = z^p \quad (p \nmid xyz) \tag{2.53}$$

has a solution, then $p^2 \mid U_{p-1}(3, 2)$. Such a prime is called a *Wieferich prime*, and the only ones known for all $p < 6.7 \times 10^{15}$ are 1093 and 3511. It is now known that if a (≤ 89) is a prime, then $p^2 \mid U_{p-1}(a+1, a)$ whenever (2.53) is true. (See Granville and Monogan [5].) Any prime p such that $p \nmid a(a-1)$ and $p^2 \mid U_{p-1}(a+1, a)$ is called a *base-a Wieferich prime*. An extensive computer search for such primes is discussed in Dorais and Klyve [4]. Of course, much of this has been rendered moot by the proof of FLT, but it does suggest the following extension of the Wieferich primes to Lucas-Wieferich primes. We say that if p is a prime such that $p \nmid QD$ and

$$p^2 \mid U_{p-\epsilon_p}(P, Q),$$

then p is a *Lucas-Wieferich prime* with respect to the Lucas sequence $U(P, Q)$.

However, there is one class of primes for which the rank exponent can only be 1.

Theorem 12 *Suppose $p \nmid Q$ is an odd prime and either $p \geq 5$ and $p \mid D$, or $p = 3$ and $9 \mid D$. Then the rank exponent of p is 1, i.e., $p^2 \nmid U_p$.*

Proof By Theorem 9, $\rho(p) = p$. Using the identity (2.40), which expresses U_n as a polynomial in P and D, with $n = p$, we find that as $p \geq 3$,

$$2^{p-1}U_p \equiv pP^{p-1} + \binom{p}{3}P^{p-3}D \pmod{D^2}.$$

Note that $p \mid D$ and $p \nmid Q$ implies that $p \nmid P$. Since $p \mid D$ and $p \mid \binom{p}{3}$ if $p \geq 5$, and $9 \mid D$ if $p = 3$, we see that $2^{p-1}U_p \equiv pP^{p-1} \pmod{p^2}$. Therefore, $U_p \sim_p p$. □

Remark 14 We observe that Theorem 12 does not hold for $p = 2$, or $p = 3$ and $9 \nmid D$. For instance, if $P = 4$ and Q is odd, we find that $2 \mid D$, but $2^2 \mid U_2$. For $p = 3$, $P = 10$, and $Q = 1$, we obtain that $3 \mid D$ and $U_3 = 99$. Thus, the rank exponent of 3 is 2.

Remark 15 If $Q = 1$ and $D = 0$, then all primes $p \geq 3$ satisfy the hypotheses of Theorem 12. But then either $U_n = I_n = n$ for all n, or $U_n = (-1)^n I_n$ for all n, and the rank exponent is trivially seen to be 1.

It remains to look at the appearance of powers of 2 in U, a case not addressed by the lifting-the-exponent lemma. We proceed to complete the picture in the next section.

2.5 Divisibility of U_n by Powers of 2

The case when 2 is a special prime is fully addressed in Sect. 2.12. For now, we are content to observe, by Lemma 1, that, in that case and that case only, all terms U_n, $n \geq 2$, are even.

If $2 \mid Q$ and $2 \nmid P$, then as mentioned in Lemma 1, all U_n, $n \geq 1$, are odd.

Thus, we are mainly interested in the case $2 \nmid Q$. We state two distinct theorems depending on the parity of P.

Theorem 13 *Suppose Q is odd and P is even. Then for all $n \geq 0$,*

$$U_{2n+1} \sim 1 \quad \textit{and} \quad U_{2n} \sim nU_2 = nP \quad (\textit{base } 2).$$

Theorem 14 *Suppose P and Q are odd. Then $\rho(2) = 3$, and, for all $n \geq 0$, we have*

$$4 \mid U_3 \quad \text{and} \quad U_{3n} \sim nU_3 \quad (\text{base } 2), \qquad \text{if } Q \equiv 1 \pmod 4,$$

and

$$2 \,||\, U_{6n+3},\ 8 \mid U_6 \quad \text{and} \quad U_{6n} \sim nU_6 \quad (\text{base } 2), \qquad \text{if } Q \equiv -1 \pmod 4.$$

We begin with a few lemmas useful in proving both theorems.

Lemma 12 *Suppose Q is odd. If $V_s \sim_2 2$, for some $s \geq 0$, then $V_{ns} \sim_2 2$ for all $n \geq 0$.*

Proof If $n = 0$, then $V_{ns} = V_0 = 2$, and the lemma holds. If $n \geq 1$, then write $n = (2h+1)2^u$. If $u \geq 1$, then, as $V_s \mid V_{(2h+1)s}$, $V_{(2h+1)s}$ is even. Note that if $2 \mid V_t$, then $2 \,||\, V_{2t}$ because $V_{2t} = V_t^2 - 2Q^t$ and Q is odd. Thus, we see inductively that $2 \,||\, V_{2^u(2h+1)s} = V_{ns}$. If $u = 0$, then n is odd, and we at least know that V_{ns} is even. Moreover, by the addition formula (2.11),

$$2V_{ns} = 2V_{(2h+1)s} = 2V_{2hs+s} = V_{2hs}V_s + DU_{2hs}U_s.$$

By Lemma 1, when Q is odd, U_ℓ is even iff V_ℓ is. Thus, each of the three factors in the product $U_{hs}V_{hs}U_s$ is even for all h. Hence, $\nu_2(DU_{2hs}U_s) \geq \nu_2(U_{hs}V_{hs}U_s) \geq 3$. However, since $2h$ is even, $\nu_2(V_{2hs}V_s) = 1 + 1 = 2$. Therefore, $\nu_2(2V_{ns}) = \nu_2(V_{2hs}V_s) = 2$ so that $\nu_2(V_{ns}) = 1$. □

Lemma 13 *Suppose Q is odd. If $2 \mid U_s$, then*

$$U_{ns} \sim U_s \quad (\text{base } 2), \text{ for all odd } n \geq 1.$$

Proof Note first that V_s is even, whatever the parity of P, by Lemma 1. We reason inductively. The lemma clearly holds for $n = 1$. Suppose it holds for some odd $n \geq 1$. We proceed to show it holds for $n + 2$. Using the addition formula (2.10), we see that

$$2U_{(n+2)s} = 2U_{ns+2s} = U_{ns}V_{2s} + U_{2s}V_{ns}.$$

By the inductive hypothesis, $\nu_2(U_{ns}) = \nu_2(U_s)$ and $\nu_2(V_{2s}) = 1$ since $V_{2s} = V_s^2 - 2Q^s$ and V_s is even. Hence, $\nu_2(U_{ns}V_{2s}) = 1 + \nu_2(U_s)$, whereas $U_{2s}V_{ns} = U_sV_sV_{ns}$ has a 2-adic valuation at least $2 + \nu_2(U_s)$ since $V_s \mid V_{ns}$. Therefore, $\nu_2(2U_{(n+2)s}) = 1 + \nu_2(U_s)$. That is, $\nu_2(U_{(n+2)s}) = \nu_2(U_s)$. □

Lemma 14 *Suppose Q is odd. If $2 \mid U_s$ and $2 \,||\, V_s$, then for all integers $n \geq 0$,*

$$U_{ns} \sim nU_s \quad (\text{base } 2).$$

Proof We prove the lemma by induction on $\nu_2(n)$. The base step of our induction holds by Lemma 13, i.e., for all odd integers n.

Suppose $U_{ns} \sim_2 nU_s$ for all integers $n \geq 1$ with dyadic valuation k for some $k \geq 0$. Let $m \geq 1$ be an integer with $\nu_2(m) = k+1$, and write $m = 2n$. By Lemma 12, $2 \,||\, V_{ns}$. Therefore,

$$U_{ms} = U_{2ns} = V_{ns}U_{ns} \sim 2 \cdot nU_s = mU_s \quad \text{(base 2)}, \tag{2.54}$$

and our induction is complete. □

Proof of Theorem 13. As already observed in Lemma 1, $2 \mid U_n$ if and only if $2 \mid n$. Thus, $U_{2n+1} \sim_2 1$. To see that $U_{2n} \sim_2 nU_2$, it suffices to apply Lemma 14 with $s = 2$. Indeed, $2 \,||\, V_2$ since $V_2 = P^2 - 2Q \equiv 2 \pmod 4$.

Proof of Theorem 14. By Lemma 1, X_n is even if and only if $3 \mid n$, where X stands for either U or V.

Case 1. $Q \equiv 1 \pmod 4$. Then $U_3 = P^2 - Q \equiv 0 \pmod 4$ and $V_3 = P(P^2 - 3Q) \equiv 2 \pmod 4$. Thus, $U_{3n} \sim_2 nU_3$ for all $n \geq 1$ by Lemma 14 with $s = 3$.

Case 2. $Q \equiv -1 \pmod 4$. Then $U_3 = P^2 - Q \equiv 2 \pmod 4$ so $2 \,||\, U_3$. By Lemma 13, $U_{(2n+1)3} \sim_2 U_3$, so $2 \,||\, U_{6n+3}$. Now $P^2 - 3Q \equiv 0 \pmod 4$ so $4 \mid V_3 = P(P^2 - 3Q)$. Hence, $8 \mid U_6 = U_3V_3$. Also, $2 \,||\, V_6 = V_3^2 - 2Q^3$.

Applying Lemma 14 with $s = 6$ yields $U_{6n} \sim_2 nU_6$ for all $n \geq 1$.

Remark 16 In the case $Q \equiv -1 \pmod 4$, there is a jump equal to

$$\nu_2(P^2 - 3Q) \geq 2$$

between the 2-adic valuations of U_3 and U_6 larger than the expected jump of 1 coming from the fact that $6 = 2 \times 3$. But starting from U_6, the increase in the 2-adic valuation of U_{6n} is again governed by $\nu_2(n)$, the 2-adic valuation of n.

Remark 17 We note in passing that Theorem 13 can be proved directly using the polynomial expression (2.31) for U_n. Indeed,

$$U_{2n+1} = \sum_{k=0}^{n} (-1)^k \binom{2n-k}{k} P^{2n-2k} Q^k,$$

and the only odd term in this sum is $(-Q)^n$ obtained when $k = n$. Thus, $U_{2n+1} \sim_2 1$. Also, from (2.31), we see that

$$U_{2n} = \sum_{k=0}^{n-1} (-1)^k \binom{2n-k-1}{k} P^{2n-2k-1} Q^k,$$

from what we might suspect the term $(-1)^{n-1} nPQ^{n-1} \sim_2 nP = nU_2$, obtained when $k = n-1$, to have the lowest 2-adic valuation of all terms. This inkling was proved in [2, p. 273], putting $a = \nu_2(P) > 0$ and $b = \nu_2(Q) = 0$.

Using Theorems 13 and 14, we state a corollary analogous to Corollary 11.

Corollary 15 Suppose $2 \nmid Q$. Let ρ and ν, respectively, denote the rank and the rank exponent of 2. If P is even or if $Q \equiv 1 \pmod 4$, then

$$\rho(2^a) = \begin{cases} \rho, & \text{if } 1 \le a \le \nu; \\ 2^{a-\nu}\rho, & \text{if } a \ge \nu. \end{cases}$$

If P is odd and $Q \equiv -1 \pmod 4$, then, with $\nu_* = \nu_2(U_6) = 1+\nu_2(P^2-3Q) \ge 3$, we find that

$$\rho(2^a) = \begin{cases} 3, & \text{if } a = 1; \\ 6, & \text{if } 2 \le a \le \nu_*; \\ 2^{a-\nu_*} \cdot 6, & \text{if } a \ge \nu_*. \end{cases}$$

2.6 Composite Integers Dividing U and Their Rank

By Lemma 8, we know all integers prime to Q admit a rank of appearance. Also, from Theorem 8, given an integer $m \ge 2$ prime to Q, we know m divides U_n if and only if n is a multiple of the rank of m. Moreover, if some prime factor of m divides Q, but not P, then by Lemma 6, no U_n, with $n \ge 1$, is divisible by m. We have gathered information on the rank of primes and prime powers in the previous two sections. We now state a theorem on the rank of m, m prime to Q, in terms of the ranks of its prime factors.

Theorem 16 *Let $m \ge 2$ be an integer prime to Q of rank ρ in $U(P,Q)$. If $m = \prod_{i=1}^{r} p_i^{a_i}$, then*

$$\rho = \operatorname{lcm}\left(\rho(p_1^{a_1}),\ \rho(p_2^{a_2}), \ldots,\ \rho(p_r^{a_r})\right).$$

Proof Let M be the least common multiple of the ranks $\rho(p_i^{a_i})$, $1 \le i \le r$. By Theorem 8,

$$m \mid U_n \iff \rho \mid n.$$

But $m \mid U_n$ if and only if $p_i^{a_i} \mid U_n$ for all $1 \le i \le r$. Hence, by Theorem 8 again,

$$\begin{aligned} m \mid U_n &\iff \rho(p_i^{a_i}) \mid n \quad (\text{all } i,\ 1 \le i \le r) \\ &\iff M \mid n. \end{aligned}$$

Hence, $\rho = M$, i.e., M is the rank of m. □

Example 17 With respect to the Fibonacci sequence, $\rho(3) = 4$ and $\rho(7) = 8$ so $\rho(21) = \operatorname{lcm}(4,8) = 8$. Indeed, $F_8 = 21$. □

Application 18 Prove that for all $n \geq 1$, $P_n^2 \mid P_m$ iff $nP_n \mid m$, where $P = U(2, -1)$ is the so-called Pell sequence. Suppose $\prod_{p^a \,||\, P_n} p^a$ is the prime factorization of P_n. Note that if $p^a \,||\, P_n$, then $a \geq \nu$, where ν is the rank exponent of p. By Theorem 16 and Corollaries 11 and 15,

$$\rho(P_n) = \text{lcm}_{p^a \,||\, P_n} \big(\rho(p^a)\big) = \Big(\prod_{p|P_n} p^{a-\nu}\Big) \cdot \text{lcm}_{p|P_n} \big(\rho(p)\big).$$

Hence,

$$\begin{aligned} \rho(P_n^2) &= \Big(\prod_{p|P_n} p^{2a-\nu}\Big) \cdot \text{lcm}_{p|P_n} \big(\rho(p)\big) \\ &= \Big(\prod_{p|P_n} p^a\Big) \cdot \Big(\prod_{p|P_n} p^{a-\nu}\Big) \cdot \text{lcm}_{p|P_n} \big(\rho(p)\big) \\ &= P_n \cdot \rho(P_n) = P_n \cdot n. \end{aligned}$$

Indeed, the fact that for $n \geq 2$, $P_n > 1$ and P_n is an increasing function of n implies that $\rho(P_n) = n$. Hence, $P_n^2 \mid P_m$ if and only if $nP_n \mid m$, by Theorem 8. The case $n = 1$ is trivial to check. (If $n \geq 3$, then $F_n^2 \mid F_m$ iff $nF_n \mid m$, where F_k designates the kth Fibonacci number. This property is a lemma famously used by Matijasevich in his solution to Hilbert's tenth problem.) □

2.7 Divisibility of V_n by Powers of an Odd Prime

If $\{U, V\}$ is a pair of Lucas sequences, then, while all primes not dividing Q divide some terms of U, there are usually infinitely many primes which do not divide any term of the companion sequence V. Actually, the infinite collection of primes which do not divide any V_n represents a positive "proportion" of the primes. Precise theorems on the size of the set of primes that divide a companion Lucas sequence will be stated in Chap. 9.

As an example, consider the sequence of Lucas numbers L, where $L_n = V_n(1, -1)$. We find that modulo 5

$$L: \quad 2, 1, 3, 4, 2, 1, \ldots$$

That is, $L \pmod 5$ has period 4, and the residue 0 (mod 5) never appears. Thus, for all $n \geq 0$, $5 \nmid L_n$. Similarly, for $p = 13$, we find that modulo 13

$$L: \quad 2, 1, 3, 4, -6, -2, 5, 3, -5, -2, 6, 4, -3, 1, -2, -1, \ldots$$

Since $L_{14} \equiv -L_0 = -2 \pmod{13}$ and $L_{15} \equiv -L_1 = -1 \pmod{13}$ and $13 \nmid L_n$ for $0 \leq n \leq 13$, there can never be a value of $n \geq 0$ such that $13 \mid L_n$.

In fact, in 1985, Lagarias [9] showed that on average, exactly one out of three primes does not divide any Lucas number.

Let us begin by defining the *V-rank* of a generic integer m.

Definition 3 (V-rank) Let $m \geq 2$ be an integer. We define the V-rank of m, or the rank of appearance of m in V, denoted as σ, or $\sigma(m)$, to be, if it exists, the least positive index t such that $m \mid V_t$. We may occasionally use the alternate notation ρ_V or $\rho_V(m)$.

We are about to see that for all primes not dividing $2Q$, there is a very simple criterion for the V-rank to exist.

Theorem 19 *Let $p \nmid 2Q$ be a prime of rank ρ. Let σ denote the V-rank of p. Then*

$$\sigma \text{ exists} \quad \Longleftrightarrow \quad \rho \text{ is even},$$

in which case $\sigma = \rho/2$. Moreover, the p-adic valuations of U_ρ and V_σ are the same.

Proof We begin with the proof of the converse. Thus, we suppose ρ is even, say $\rho = 2\rho^*$. Then $p \nmid U_{\rho^*}$, but $p \mid U_\rho$. Since by (2.23) $U_\rho = U_{\rho^*} V_{\rho^*}$, p must divide V_{ρ^*}. Thus, $\sigma \leq \rho^*$ exists. Moreover, by (2.23) again, as $p \mid V_\sigma$, $p \mid U_{2\sigma}$. Hence, $\rho \mid 2\sigma$. That is, $\rho^* \mid \sigma$. Thus, $\sigma = \rho^*$.

Now assume that σ exists. Then $p \mid V_\sigma$ implies that $p \mid U_{2\sigma}$. Hence, $\rho \mid 2\sigma$. By Lemma 3 and since $p \nmid 2Q$, $p \nmid \gcd(U_\sigma, V_\sigma)$. So $p \nmid U_\sigma$. But $\rho \mid 2\sigma$ and $\rho \nmid \sigma$ says that ρ is even. (Therefore, by the proof of the converse, $\sigma = \rho/2$.)

That $U_\rho \sim_p V_\sigma$ follows from the identity $U_\rho = U_\sigma V_\sigma$ and $p \nmid U_\sigma$. □

It is easy to verify that 5 and 13 are the least two primes with no L-rank, where $L = V(1, -1)$. Their respective ranks in $F = U(1, -1)$, 5 and 7, are indeed odd.

Theorem 19 also holds for prime powers. That is, the V-rank of the power of a prime p not dividing $2Q$ exists if and only if the rank of this prime power is even. This occurs if and only if $\sigma(p)$ exists.

Corollary 20 Let $p \nmid 2Q$ be a prime of rank ρ and rank exponent ν. Suppose $a \geq 1$ is an integer. Then

$$\sigma(p^a) \text{ exists} \quad \Longleftrightarrow \quad \rho \text{ is even}.$$

Moreover, if ρ is even, then

$$\sigma(p^a) = \frac{1}{2}\rho_U(p^a) = \frac{1}{2}\rho p^{(a-\nu)[a>\nu]},$$

where $[-]$ denotes the Iverson symbol. Also, the p-adic valuations of $U_{\rho(p^a)}$ and $V_{\sigma(p^a)}$ are equal. □

Proof We can clone the proof of Theorem 19, once we observe, by Corollary 11, that $\rho(p^a) = \rho p^\ell$, where $\ell := (a - \nu)[a > \nu]$, and thus that ρ is even if and only if $\rho(p^a)$ is even. □

Alternatively, we can state part of the previous result in the manner of Corollary 11, as follows:

Corollary 21 Suppose $p \nmid 2DQ$ is a prime and $\sigma(p)$ exists. Then

$$\sigma(p^a) = \begin{cases} \sigma, & \text{if } 1 \le a \le \nu; \\ p^{a-\nu}\sigma, & \text{if } a > \nu, \end{cases}$$

where $p^\nu \,||\, V_\sigma$. □

Odd primes p dividing D have no V-rank by Theorem 9 since their rank ρ, equal to p, is odd. Hence, they are excluded twice from consideration in the statement of Corollary 21.

For the powers of an odd prime with even rank, we may state a law of regular division analogous to Theorem 8.

Theorem 22 *Given a prime $p \nmid 2Q$ of even rank and an integer $a \ge 1$, we have for all $n \ge 1$*

$$p^a \mid V_n \iff n = (2k+1)\sigma(p^a),$$

for some $k \ge 0$.

Proof By the double-angle formula (2.23) and Lemma 4, $p^a \mid V_n$ implies that $p^a \mid U_{2n}$, but $p^a \nmid U_n$. Hence, $\rho(p^a) \mid 2n$, but $\rho(p^a) \nmid n$. Since, by Corollary 20, $\rho(p^a) = 2\sigma(p^a)$, we see that $\sigma(p^a) \mid n$, but $2\sigma(p^a) \nmid n$. It follows that n is an odd multiple of $\sigma(p^a)$.

For the converse, we only need to invoke Theorem 4. □

Corollary 23 Suppose $p \nmid 2Q$ is prime and m and n are positive integers. Then

$$m \sim_2 n \implies \gcd(V_m, V_n) \sim_p V_{\gcd(m,n)}.$$

Proof Say $p^a \mid \gcd(V_m, V_n)$. Then, by Theorem 22, $m = (2k+1)\sigma(p^a)$ and $n = (2\ell+1)\sigma(p^a)$ for some nonnegative k and ℓ. Thus, $\sigma(p^a)$ divides $\gcd(m, n)$ and $\sigma(p^a) \sim_2 m \sim_2 n \sim_2 \gcd(m, n)$. Therefore, by Theorem 4, $p^a \mid V_{\gcd(m,n)}$. If $p^a \mid V_{\gcd(m,n)}$, then, by Theorem 4, p^a divides both V_m and V_n since m and n are odd multiples of $\gcd(m, n)$. □

Regular primes dividing Q cannot divide any U term, so they cannot divide any V term by the double-angle formula. Thus, we now turn to the divisibility of V terms by powers of 2.

2.8 Divisibility of V_n by Powers of 2

The parity of V terms was given in Lemma 1. But the behavior of the prime 2, when $2 \nmid Q$, is radically different from the behavior of odd primes $p \nmid Q$. Indeed, by Corollary 20, if p is odd and $\sigma(p)$ exists, then powers of p in V are unbounded. On the contrary, powers of 2 always remain bounded in a companion Lucas sequence, at least in the nondegenerate case.

Theorem 24 *Suppose Q is odd. If P is even, then, for all $n \geq 0$,*

$$V_{2n} \sim 2 \quad \textit{and} \quad V_{2n+1} \sim P \quad (\textit{base } 2).$$

If P is odd, then we have $2 \mid V_t \iff 3 \mid t$. Moreover, for $n \geq 0$,

$$V_{3(2n+1)} = V_{6n+3} \sim V_3 \sim P^2 - 3Q \quad \textit{and} \quad V_{6n} \sim 2 \quad (\textit{base } 2).$$

Proof Suppose P is even. By Theorem 13,

$$U_{2n+1} \sim_2 1 \quad \text{and} \quad U_{4n+2} \sim_2 (2n+1)P \sim_2 P.$$

Since $V_{2n+1}U_{2n+1} = U_{4n+2}$, we have $V_{2n+1} \sim_2 U_{4n+2} \sim_2 P$. Also, $V_2 = P^2 - 2Q \sim_2 2$ so that, by Lemma 12, $V_{2n} \sim_2 2$ for all $n \geq 0$.

Now suppose that P is odd. That $2 \mid V_t$ iff $3 \mid t$ was already observed in Lemma 1. Since $V_3 = P(P^2 - 3Q)$ and P is odd, $V_3 \sim_2 P^2 - 3Q$. Thus, if $Q \equiv 1 \pmod 4$, then $P^2 - 3Q \equiv 1 + Q \equiv 2 \pmod 4$, so $V_3 \sim_2 2$. By Lemma 12, $V_{3n} \sim_2 2$ for all $n \geq 0$. Suppose $Q \equiv -1 \pmod 4$. By Theorem 14,

$$U_{3(2n+1)} \sim_2 2 \quad \text{and } U_{6(2n+1)} \sim_2 (2n+1)U_6.$$

In particular, $U_3 \sim_2 2$. Therefore,

$$2V_3 \sim U_3V_3 = U_6 \sim U_{6(2n+1)} = U_{3(2n+1)}V_{3(2n+1)} \sim 2V_{3(2n+1)} \quad (\text{base } 2).$$

This implies $V_{3(2n+1)} \sim_2 V_3$.

Again, by Theorem 14, $U_{6n} \sim_2 nU_6$. Hence,

$$2nU_6 \sim U_{12n} = U_{6n}V_{6n} \sim nU_6V_{6n} \quad (\text{base } 2),$$

from which we see that $V_{6n} \sim_2 2$. □

Remark 18 The 2-adic valuation of V is simplest in two cases. If Q is odd and $P \equiv 2 \pmod 4$, then $V_n \sim_2 2$ for all $n \geq 0$. If PQ is odd with $Q \equiv 1 \pmod 4$, then $V_n \sim_2 2$, if $3 \mid n$, and $V_n \sim_2 1$, if $3 \nmid n$.

We rephrase Theorem 24 as a law of appearance for powers of 2 in the next corollary. Note that Equation (2.55) is reminiscent of Theorem 22.

Corollary 25 Suppose Q is odd. Then, for $a \geq 2$,

$$\sigma(2^a) = \begin{cases} 1, & \text{if } 4 \mid P \text{ and } a \leq \nu_2(P); \\ 3, & \text{if } P \text{ is odd, } Q \equiv -1 \pmod 4 \text{ and } a \leq \nu_2(P^2 - 3Q), \end{cases}$$

and

$$2^a \mid V_n \iff n = (2k+1)\sigma(2^a), \tag{2.55}$$

for some $k \geq 0$. Moreover, if a exceeds, respectively, $\nu_2(P)$ or $\nu_2(P^2 - 3Q)$, then $\sigma(2^a)$ does not exist.

To complete the picture, we have for P even:
$2 \,||\, V_n$ for all $n \geq 0$ if $P \equiv 2 \pmod 4$ or if n is even and $4 \mid P$.
For P odd, we have:
$2 \,||\, V_{3n}$ for all $n \geq 0$ if $Q \equiv 1 \pmod 4$ or if n is even and $Q \equiv -1 \pmod 4$.

A result similar to Corollary 23 can be proved with respect to $p = 2$.

Corollary 26 Suppose Q is odd and m and n are positive integers. Then

$$m \sim_2 n \implies \gcd(V_m, V_n) \sim_2 V_{\gcd(m,n)}.$$

Proof We use Theorem 24 throughout. Say $2^a \mid \gcd(V_m, V_n)$. Then $a \leq M$, where

$$M := \nu_2(P) \cdot [2 \mid P] + \nu_2(P^2 - 3Q) \cdot [2 \nmid P] \geq 1. \tag{2.56}$$

If $a \geq 2$, then we can, using (2.55), carry out the same reasoning as in the proof of Corollary 23 to prove our result. So assume $a \leq 1$. If $P \equiv 2 \pmod 4$, then all V_t, $t \geq 0$, have 2-adic valuation 1. So the result holds. If $4 \mid P$, then we only need to consider the case where m and n are both even; otherwise, $a \geq 2$. Thus, $a = 1$. Hence, $2 \,||\, V_{\gcd(m,n)}$ because $\gcd(m, n)$ is even. So the result is true. Suppose P is odd. When $Q \equiv 1 \pmod 4$, all even V terms have 2-adic valuation equal to 1. Since V_t is even iff $3 \mid t$, we see that $2 \,||\, \gcd(V_m, V_n)$ iff $3 \mid \gcd(m, n)$, which occurs iff $2 \,||\, V_{\gcd(m,n)}$. If $Q \equiv -1 \pmod 4$, then $2 \,||\, V_{\gcd(m,n)}$ iff $6 \mid \gcd(m, n)$, which occurs iff V_m and V_n are both even with 2-adic valuation 1. □

Remark 19 It may be observed that if $4 \mid V_n$ for some $n \geq 1$, then $2^M \,||\, V_n$, where M was defined in (2.56). In fact, n is an odd multiple of $\sigma(4) = \sigma(2^M)$.

2.9 Composite Integers Dividing V

We are now concerned with integers $m \geq 2$ that are divisors of a companion Lucas sequence V, i.e., such that $m \mid V_n$ for some $n \geq 1$, which we write $m \mid V$. As mentioned earlier, the set of primes which do not divide V not only is most often infinite but contains a positive proportion of the primes. Therefore, the set of integers whose prime factors all divide V must have a 0-asymptotic density within the set of integers. A fortiori, if D_V denotes

the divisor set of V, i.e., if $D_V := \{m;\ m \mid V\}$, then $\#D_V(x) = o(x)$. That is, few integers divide V. Actually, most integers with prime factors all dividing V are not in D_V as Theorem 27 will suggest. In fact, when α and β are coprime integers, $\alpha/\beta \neq \pm 1$, Moree's work [14, Theorem 5] provides estimates for $\#D_V(x)$. In particular, if $\alpha/\beta \notin \mathbb{Q}^2$, then $\#D_V(x)$ is asymptotically equivalent to $cx/\log^{2/3} x$ for some positive constant c, as $x \to \infty$. The next theorem gives an idea of how stringent conditions are for a generic integer to divide a companion Lucas sequence.

Theorem 27 *Suppose $m \geq 3$, $\gcd(m, Q) = 1$, and $m = 2^a \prod_{i=1}^{s} p_i^{b_i}$ is the factorization of m into prime factors $2 < p_1 < p_2 < \cdots < p_s$, where $a \geq 0$, $s \geq 0$, and $b_i \geq 1$. Let ρ_i denote the rank of p_i and $p_i^{\nu_i} \,||\, U_{\rho_i}$. Then $\sigma(m)$, the V-rank of m, exists if and only if the three conditions below are satisfied:*

- $\nu_2(\rho_1) = \nu_2(\rho_2) = \cdots = \nu_2(\rho_s) := \nu_* \geq 1$,
- $a \leq \begin{cases} \nu_2(P), & \text{if } P \text{ is even;} \\ \nu_2(P^2 - 3Q), & \text{if } P \text{ is odd,} \end{cases}$
- $\nu_* = 1$, *if* $a \geq 2$.

In case of existence,

$$\sigma(m) = \frac{1}{2} \operatorname{lcm}(\rho_0, \rho_1 p_1^{e_1}, \rho_2 p_2^{e_2}, \ldots, \rho_s p_s^{e_s}), \tag{2.57}$$

where

$$\rho_0 = \begin{cases} 6, & \text{if } P \text{ is odd and } a > 0; \\ 2, & \text{otherwise,} \end{cases}$$

and $e_i = \max\{0, b_i - \nu_i\}$. Moreover, for all $n > 0$,

$$m \mid V_n \iff n = (2k+1)\sigma(m), \quad \text{for some } k \geq 0.$$

Proof The existence of a $\nu_* \geq 1$ such that

$$\nu_* = \nu_2(\rho_1) = \nu_2(\rho_2) = \cdots = \nu_2(\rho_s) \tag{2.58}$$

is necessary for $\sigma(m)$ to exist. Indeed, m divides V implies all its odd prime factors divide V. But by Theorem 19, p_i divides V iff ρ_i is even. Note that, by Corollary 21, $p \mid V$ implies $p^b \mid V$ for all $b \geq 1$. Now, in order to find an $n \geq 1$ such that all $p_i^{b_i}$ simultaneously divide V_n, n must be an odd multiple of all $\sigma(p_i^{b_i})$. But $\sigma(p_i^{b_i}) \sim_2 \sigma(p_i)$. Hence, all $\sigma(p_i)$ must have the same 2-adic valuation. Since $\rho(p_i) = 2\sigma(p_i)$, there is an $\nu_* \geq 1$ such that (2.58) holds. If m is odd, or if m is even with $a = 1$ and P even, in which case $2 \mid V_n$ for all n, then the condition (2.58) is sufficient. Moreover, n is an odd multiple of all $\sigma(p_i^{b_i})$ if and only if n is an odd multiple of the least common multiple of all $\sigma(p_i^{b_i})$, which must be $\sigma(m)$. Hence, $\sigma(m)$ is given by (2.57) in those cases.

Note that if $a \geq 1$ with P odd, then $2 \mid V_n$ iff $3 \mid n$. So we must make sure that $3 \mid \sigma(m)$ which explains the presence of $\rho_0 = 6$ in (2.57). If $a \geq 2$, then, by Corollary 25, a must be bounded above either by $\nu_2(P)$, if $4 \mid P$, or by $\nu_2(P^2 - 3Q)$, if P is odd, in order to have V terms divisible by 2^a. Moreover, by (2.55), n must be an odd multiple of $\sigma(2^a)$. Since $\sigma(2^a)$ is either 1 or 3, $\sigma(2^a)$ is odd, and we must have $\nu_* = 1$ in order for m to divide V_n. □

Example 28 Consider $L = V(1, -1)$. Then $m = 8 \nmid L$ since $a = 3$, $P^2 - 3Q = 4$, and $a > \nu_2(P^2 - 3Q)$. However, $m = 4$ divides L. Here, $\rho_0 = 6$, $\sigma(4) = 3$, and $4 \mid L_n$ iff $n = 6k + 3$ for some $k \geq 0$. But $21 = 3 \cdot 7 \nmid L$ because $\rho(7) = 8$ has a 2-adic valuation greater than $\rho(3) = 4$. Now $319 = 11 \cdot 29 \mid L$, because $\rho(11) = 10$ and $\rho(29) = 14$ are both even with 2-adic valuation 1. Hence, $\sigma(319) = 35$ and $319 \mid L_{70k+35}$ for all $k \geq 0$. Similarly, $1276 = 4 \cdot 319$ divides L because $\nu_* = 1$. But $28 \nmid L$ since $\nu_* = \nu_2(\rho(7)) = 3 > 1$. □

We state a corollary of Theorem 27, which is only a particular case of that theorem, but with a simpler statement.

Corollary 29 Suppose $m \geq 3$, coprime to Q, is either odd or such that $2 \,||\, m$ and has $s \geq 1$ odd prime factors $p_1, \ldots, p_s$. Let ρ_i denote the rank of p_i. Then

$$\sigma(m) \text{ exists} \iff \nu_2(\rho_1) = \nu_2(\rho_2) = \cdots = \nu_2(\rho_s) \geq 1,$$

where, in case of existence, $\sigma(m) = \frac{\rho(m)}{2}$. Moreover, for all $n > 0$,

$$m \mid V_n \iff n = (2k+1)\sigma(m), \quad \text{for some } k \geq 0.$$

Remark 20 We observe that if m admits a V-rank $\sigma(m)$, then, in fact, we always find that

$$\sigma(m) = \frac{\rho(m)}{2}.$$

Indeed, if $m = 2^a b$, b odd, $2 \leq a \leq M$, where M was defined in (2.56), then

$$\rho(2^a) = \begin{cases} 2, & \text{if } 2 \mid P; \\ 6, & \text{if } 2 \nmid P. \end{cases}$$

Hence, $\rho(m) = \operatorname{lcm}(\rho(2^a), \rho(b)) = 2\operatorname{lcm}(\sigma(2^a), \sigma(b)) = 2\sigma(m)$.

The next result is a combination of Corollaries 23 and 26.

Corollary 30 Let $p \nmid Q$ be a prime and m and n be two positive integers. Then

$$m \sim_2 n \implies \gcd(V_m, V_n) \sim_p V_{\gcd(m,n)}.$$

Before ending the section, we single out, without proof, a few corollaries which are immediate consequences of the preceding theorems.

Corollary 31 If $m \geq 3$, $\gcd(m, Q) = 1$, then

$$m \mid V_n \implies 2 \nmid \frac{n}{\sigma(m)}.$$

Corollary 32 If ℓ is a product of regular primes and $\ell \mid V_m$, then

$$n \not\sim_2 m \implies \gcd(\ell, V_n) = 1.$$

Corollary 33 If $\ell_1 \mid V_m$ and $\ell_2 \mid V_n$, where $m \sim_2 n$ and $\gcd(\ell_1, \ell_2) = 1$, then $\ell_1 \ell_2 \mid V_{\text{lcm}(m,n)}$. □

Corollary 34 If $\ell_1 \mid V_m$ and $\ell_2 \mid V_n$ with $m \not\sim_2 n$, $\ell_1 \geq 3$, $\ell_2 \geq 3$, and $\gcd(\ell_1 \ell_2, Q) = 1$, then $\ell_1 \ell_2 \nmid V_k$ for all $k \geq 0$. □

Corollary 35 If $m \geq 3$, $\gcd(m, Q) = 1$, and $2 \nmid \rho(m)$, then $\sigma(m)$ cannot exist. □

2.10 Euler's Criterion for Lucas Sequences

Euler's criterion says that if p is an odd prime and a is an integer prime to p, then a is a square modulo p if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. That is, if U is the Lucas sequence with parameters $P = a + 1$ and $Q = a$, then the rank $\rho_U(p)$ divides $\frac{p-1}{2}$, halfway through the maximal potential rank $p - 1$. The next theorem, much as the law of appearance generalized Fermat's little theorem, generalizes the classical Euler criterion. Interestingly, it is also valid when $\epsilon_p = -1$, where ϵ_p was defined in (2.52). In the sequel, $(Q \mid p)$ denotes the Legendre character of Q modulo p.

Theorem 36 (Euler's criterion for Lucas sequences) *Suppose U is a fundamental Lucas sequence with parameters P and Q and p is a prime not dividing $2QD$. Then*

$$p \mid U_{\frac{p-\epsilon_p}{2}} \iff (Q \mid p) = 1.$$

We begin with two lemmas.

Lemma 15 *If $p \nmid 2QD$ is prime, then*

$$V_{p-\epsilon_p} \equiv 2Q^{\frac{1-\epsilon_p}{2}} \pmod{p}.$$

Proof As $p \nmid D$, $\epsilon_p = \pm 1$.

Case 1. $\epsilon_p = 1$**.** Using the subtraction formula (2.13), we see that

$$2QV_{p-1} = V_p V_1 - DU_p U_1 \equiv P^2 - D = 4Q \pmod{p},$$

where the congruence is obtained with the help of Lemma 9. This yields $V_{p-1} \equiv 2 \pmod{p}$. (Alternatively, when $\epsilon_p = 1$, we may view $\alpha \pmod{p}$ and $\beta \pmod{p}$ as belonging to the finite field $\mathbb{F}_p$. Thus, $V_{p-1} = \alpha^{p-1} + \beta^{p-1} \equiv 1 + 1 = 2 \pmod{p}$.)

Case 2. $\epsilon_p = -1$**.** Using the addition formula (2.11) and Lemma 9, we find that

$$2V_{p+1} = V_p V_1 + DU_p U_1 \equiv P^2 - D = 4Q \pmod{p},$$

yielding $V_{p+1} \equiv 2Q \pmod{p}$. (An alternate way of seeing this is that, by Remark 9, we have

$$V_{p+1} = \alpha^{p+1} + \beta^{p+1} = \alpha\alpha^p + \beta\beta^p \equiv \alpha\beta + \beta\alpha = 2Q \pmod{p}.)$$

Lemma 16 *If $p \nmid 2QD$ is prime, then*

$$(Q \mid p) = -1 \iff p \mid V_{\frac{p-\epsilon_p}{2}}.$$

Proof Using identity (2.24) and Lemma 15, we have

$$\begin{aligned} V^2_{\frac{p-\epsilon_p}{2}} &= V_{p-\epsilon_p} + 2Q^{\frac{p-\epsilon_p}{2}} \\ &\equiv 2Q^{\frac{1-\epsilon_p}{2}} + 2Q^{\frac{p-\epsilon_p}{2}} \\ &\equiv 2Q^{\frac{1-\epsilon_p}{2}}\left(1 + Q^{\frac{p-1}{2}}\right) \pmod{p}, \end{aligned}$$

which yields the lemma since $Q^{\frac{p-1}{2}} \equiv (Q \mid p) \pmod{p}$. □

Proof of Theorem 36. By the law of appearance for primes, $p \mid U_{p-\epsilon_p}$. But $U_{p-\epsilon_p} = U_{\frac{p-\epsilon_p}{2}} V_{\frac{p-\epsilon_p}{2}}$, and p cannot divide both $U_{\frac{p-\epsilon_p}{2}}$ and $V_{\frac{p-\epsilon_p}{2}}$ by Lemma 3. Hence, $p \mid U_{\frac{p-\epsilon_p}{2}}$ if and only if $p \nmid V_{\frac{p-\epsilon_p}{2}}$, which occurs, since $p \nmid Q$, if and only if $(Q \mid p) = 1$, by Lemma 16.

Remark 21 Here is a direct proof of this criterion using algebraic number theory. If $\epsilon_p = 1$, then $\alpha \pmod{p}$ and $\beta \pmod{p}$ belong to $\mathbb{F}_p$. Thus, both $\alpha^{\frac{p-1}{2}}$ and $\beta^{\frac{p-1}{2}}$ are in $\{\pm 1\}$. Hence, $Q^{\frac{p-1}{2}} = \alpha^{\frac{p-1}{2}}\beta^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ iff $\alpha^{\frac{p-1}{2}} \equiv \beta^{\frac{p-1}{2}} \pmod{p}$, which holds, as $p \nmid D$, iff $p \mid U_{\frac{p-1}{2}}$. If $\epsilon_p = -1$, then the non-trivial automorphism σ of $\mathbb{Q}(\alpha)/\mathbb{Q}$ sends $\alpha \mapsto \beta$. As seen in Remark 9, $Q \equiv \alpha^{p+1} \equiv \beta^{p+1} \pmod{p\mathcal{O}}$. Thus, $(Q \mid p) = 1$ iff both $\alpha^{\frac{p+1}{2}}$ and $\beta^{\frac{p+1}{2}}$ are in $\mathbb{F}_p$. Hence, $(Q \mid p) = 1$ iff $\alpha^{\frac{p+1}{2}} \equiv \sigma(\alpha^{\frac{p+1}{2}}) = \beta^{\frac{p+1}{2}} \pmod{p\mathcal{O}}$, which is true iff $p \mid U_{\frac{p+1}{2}}$.

2.11 Degenerate Lucas Sequences

Consider the terms of the Lucas sequence $U(-1, 1)$

$$0, 1, -1, 0, 1, -1, 0, 1, -1, \ \ldots\ , 0, 1, -1, \ldots$$

This sequence presents little interest. Moreover, all the terms U_{3k} are zero. It is often necessary to remove Lucas sequences having a zero term from consideration, particularly when division is involved.

Example 37 Besides $U(-1, 1)$ with $U_3 = 0$, the terms of $U(2, 2)$ are, with $k \geq 0$,

$$0, 1, 2, 2, 0, -4, -8, -8, 0, 16, 32, 32, 0, \ \ldots\ , 0, (-4)^k, 2(-4)^k, 2(-4)^k, \ldots$$

and $U_4 = 0$. Also the terms of $U(3, 3)$ are

$$0, 1, 3, 6, 9, 9, 0, -3^3, -3^4, -2 \cdot 3^4, -3^5, -3^5, \ \ldots\ ,$$
$$0, (-1)^k 3^{3k}, (-1)^k 3^{3k+1}, (-1)^k 3^{3k}, (-1)^k 2 \cdot 3^{3k+1}, (-1)^k 3^{3k+2}, (-1)^k 3^{3k+2}, \ldots$$

with $k \geq 0$. Here, the first zero term is U_6. □

Definition 4 (Degenerate Lucas sequence) We say that a Lucas sequence $U(P, Q)$ is *degenerate*, or that the pair $\{U, V\}$ is degenerate, whenever some U term with positive index is zero, i.e., if there exists an $n \geq 3$ such that $U_n = 0$.

We seek simple characterizations for degenerate Lucas sequences and begin with an easy lemma.

Lemma 17 *The only roots of unity lying in a quadratic number field have order* 1, 2, 3, 4, *or* 6.

Proof Say ζ is a primitive root of unity of order n, i.e., the least integer $k \geq 1$ such that $\zeta^k = 1$ is n. Then it is well known that the cyclotomic extension $\mathbb{Q}(\zeta)$ of $\mathbb{Q}$ has degree $\varphi(n)$, where φ is the Euler totient function. As ζ lies in a quadratic field, we need to have $\varphi(n) \leq 2$. If the prime power p^a divides n, then $p^{a-1}(p-1) \mid \varphi(n)$. Thus, the only acceptable prime factors are 2 and 3, i.e., $n = 2^a 3^b$ with $a \leq 2$ and $b \leq 1$, $n \neq 12$. □

Theorem 38 *The sequence $U(P, Q)$ is degenerate if and only if the following equivalent conditions are satisfied.*

(i) *The ratio α/β is a root of unity of order* 3, 4, *or* 6.
(ii) $U_4 U_6 = 0$.
(iii) $U_{12} = 0$.
(iv) $P^2 = Q$, $P^2 = 2Q$, *or* $P^2 = 3Q$.

Proof From (2.6) and $Q = \alpha\beta \neq 0$, we see that $U_n \neq 0$, for all $n \geq 1$ in case $\alpha = \beta$. If $\alpha \neq \beta$, then $U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$. Thus, $U_n = 0$ iff $(\alpha/\beta)^n = 1$. Since α/β belongs to the quadratic field $\mathbb{Q}(\sqrt{D})$ and is a root of unity, we see from Lemma 17 that n is limited to the values 1, 2, 3, 4, or 6. Since

$U_1 = 1$ and $U_2 = P \neq 0$, n must be 3, 4, or 6. All three possibilities occur as seen in Example 37. This proves condition (i), but also the equivalent condition $U_3U_4U_6 = 0$. But since U is a divisible sequence, $U_3 = 0$ implies $U_6 = 0$. Hence, condition (ii) is necessary and sufficient. Similarly, $U_4 = 0$ and $U_6 = 0$ each imply $U_{12} = 0$. Conversely, since U_{12} cannot be the first positive-indexed zero term of a U sequence, $U_{12} = 0$ implies U_4, or U_6 is zero. The equivalence with condition (iv) is obtained by noting that $U_3 = P^2 - Q$, $U_4 = P(P^2 - 2Q)$, and $U_6 = U_2U_3(P^2 - 3Q)$. □

Since a number of results are established under both the nondegeneracy and the regularity hypotheses, it is convenient to identify explicitly which sequences are actually excluded from consideration.

Corollary 39 There are only two regular degenerate Lucas sequences $U(P, Q)$. They correspond to $P = \pm 1$ and $Q = 1$.

□

Proof It suffices to note that in the fourth condition of Theorem 38, the two possibilities $P^2 = 2Q$, or $P^2 = 3Q$, cannot occur when $\gcd(P, Q) = 1$. The condition $P^2 = Q$ and $\gcd(P, Q) = 1$ occurs exactly for $P = \pm 1$ and $Q = 1$. □

Remark 22 Alternatively, one could prove Corollary 39 by observing first that Q must be ± 1. Indeed, if some prime p divides Q, then no U term is divisible by p. In particular, no U_n, $n > 0$, is zero.

Remark 23 Amusingly, one may obtain Lemma 17 with the laws of appearance and repetition and the Dirichlet theorem on primes in arithmetic progressions. Suppose U is degenerate and n is the least $t \geq 1$ such that $U_t = 0$. Then for all primes $p \nmid Q$, $\rho(p) \mid n$. Since $U_d \neq 0$ if $0 < d < n$, all primes p, up to finitely many exceptions, must satisfy $\rho(p) = n$. By the law of appearance, $n \mid p \pm 1$. Hence, all, but finitely many primes, lie in the two arithmetic progressions $\pm 1 \pmod{n}$. Therefore, $\varphi(n) \leq 2$, and n must be 3, 4, or 6. By the same token, a degenerate sequence cannot have a square discriminant D for then all primes, but finitely many, would be $1 \pmod{n}$. This can be easily verified: Indeed, $P^2 = Q$, $2Q$, or $3Q$ with $P^2 - 4Q = A^2$, respectively, forces $-3P^2$, $-P^2$, and $-P^2/3$ to be integral squares. However, invoking Dirichlet's theorem here is like using an elephant to kill a mosquito.

2.12 Divisibility of U_n and V_n by Powers of a Special Prime

Let $\{U, V\}$ be a pair of Lucas sequences with parameters P and Q. For p a regular prime, we know the p-adic valuation of all U and V terms: If $p \mid Q$, the p-adic valuation of all U_n and V_n with $n \geq 1$ is zero by Lemma 2. If

$p \nmid 2Q$, then Corollary 11 and Theorem 8 fully describe the p-adic valuation of all U_n, while Corollary 21 and Theorem 22 give the valuation of all V_n. If $p = 2$ and Q is odd, then Theorems 13 and 14 provide the 2-adic valuation of all U_n, and Theorem 24 informs us about the 2-adic valuation of all V terms.

We summarize these various theorems that concern regular primes in two nearly identical propositions, as they differ only in their form. But one wording is sometimes more convenient than the other.

Proposition 40 Suppose p is a regular prime. If $p \mid Q$, then $\nu_p(U_n) = 0$ for all $n \geq 1$. If $p \nmid Q$, then p admits a finite rank ρ, where

$$\rho \text{ is } \begin{cases} \text{a divisor of } p - (D \mid p), & \text{if } p \geq 3; \\ 2, & \text{if } 2 \mid P \text{ and } p = 2; \\ 3, & \text{if } P \text{ is odd and } p = 2. \end{cases}$$

Let ν be the rank exponent of $p \nmid Q$. If $p \geq 3$, or if $p = 2$, but either P is even, or P is odd and $Q \equiv 1 \pmod 4$, then

$$\nu_p(U_n) = \begin{cases} 0, & \text{if } \rho \nmid n; \\ \nu + \nu_p(n/\rho), & \text{if } \rho \mid n. \end{cases} \tag{2.59}$$

If P is odd and $Q \equiv -1 \pmod 4$, then

$$\nu_2(U_n) = \begin{cases} 0, & \text{if } 3 \nmid n; \\ 1, & \text{if } n = 6m + 3; \\ \nu_2(U_6) + \nu_2(m), & \text{if } n = 6m. \end{cases} \tag{2.60}$$

Proposition 41 Suppose p is a regular prime of rank ρ. Then for $n \geq 0$,

$$\nu_p(U_n) > 0 \text{ if and only if } \rho \text{ divides } n, \tag{2.61}$$

with the convention that $\rho = +\infty$, if $p \mid Q$.

Furthermore, if $p \geq 3$, or if $p = 2$, and either P is even, or P is odd with $Q \equiv 1 \pmod 4$, then for all $n \geq 1$,

$$\nu_p(U_{\rho n}) = \nu + \nu_p(n), \quad \text{if } p \nmid Q, \tag{2.62}$$

where ν is the rank exponent of p. If P is odd and $Q \equiv -1 \pmod 4$, then

$$\nu_2(U_{3n}) = \begin{cases} 1, & \text{if } 2 \nmid n; \\ \nu_2(P^2 - 3Q) + \nu_2(n), & \text{if } 2 \mid n. \end{cases} \tag{2.63}$$

Now we address the problem of determining the p-adic valuation of the terms of Lucas sequences when p is a special prime. Thus, we have $p^a \,||\, P$

and $p^b \,||\, Q$, where a and b are positive integers. These results appear in the paper [2], but the proofs provided here are more concise.

A lower bound for $\nu_p(U_n)$ is given in the next theorem. It implies that $\nu_p(U_n)$ tends to infinity as $n \to \infty$, a behavior that sets special primes apart from regular ones.

Theorem 42 *Suppose p is a special prime, i.e., p divides* $\gcd(P, Q)$. *Then*

$$\nu_p(U_n) \geq \left\lfloor \frac{n}{2} \right\rfloor,$$

for all $n \geq 1$.

Proof We proceed by induction on n after noting that as $U_1 = 1$ and $U_2 = P$, we clearly have $\nu_p(U_1) = 0 \geq \lfloor \frac{1}{2} \rfloor$ and $\nu_p(U_2) \geq 1 = \lfloor \frac{2}{2} \rfloor$. Suppose $n \geq 3$ and $\nu_p(U_k) \geq \lfloor \frac{k}{2} \rfloor$ for $k = n-2$ and $n-1$. Then

$$\begin{aligned} \nu_p(U_n) &\geq \min\{\nu_p(PU_{n-1}), \nu_p(QU_{n-2})\} \\ &\geq 1 + \min\{\nu_p(U_{n-1}), \nu_p(U_{n-2})\} \\ &= 1 + \left\lfloor \frac{n-2}{2} \right\rfloor = \left\lfloor \frac{n}{2} \right\rfloor. \end{aligned}$$

□

We will consider two cases: $b \geq 2a$ and $2a > b$.

Case I. $b \geq 2a$.

The p-adic valuation of U_n will be seen to contain two terms. One term, $(n-1)a$, gives a steady linear growth in terms of n; the other is the p-adic valuation of U'_n, where U' is a Lucas sequence for which p is regular.

Theorem 43 *Suppose p is a special prime with $P = p^a P'$, $Q = p^b Q'$, $p \nmid P'Q'$, and $b \geq 2a$. Then for all $n \geq 1$,*

$$\nu_p(U_n) = (n-1)a + \nu_p(U'_n) = \begin{cases} (n-1)a, & \text{if } b > 2a; \\ (n-1)a + \nu_p(U'_n), & \text{if } b = 2a, \end{cases}$$

where $U' = U(P', p^{b-2a}Q')$.

Proof By (2.30) and writing $b = 2a + c$, $(c \geq 0)$, we find that for all $n \geq 1$,

$$\begin{aligned} U_n = \Psi_n(P, Q) &= \sum_{k \geq 0} (-1)^k \binom{n-k-1}{k} P^{n-1-2k} Q^k \\ &= \sum_{k \geq 0} (-1)^k \binom{n-k-1}{k} p^{(n-1-2k)a} p^{2ka} (P')^{n-1-2k} (p^c Q')^k \\ &= p^{(n-1)a} \Psi_n(P', p^c Q') = p^{(n-1)a} U_n(P', p^c Q'). \end{aligned}$$

By Lemma 2, no term of $U(P', p^c Q')$ is divisible by p if $c \geq 1$. □

Case II. $2a > b$.

We start with the p-adic valuation of odd-indexed terms U_{2n+1}.

Theorem 44 *Suppose p is a special prime, $P = p^a P'$, $Q = p^b Q'$ with $2a > b$, and $p \nmid P'Q'$. Then, for all odd $n \geq 1$,*

$$\nu_p(U_n) = b\left\lfloor \frac{n}{2} \right\rfloor = bm, \text{ if } n = 2m+1.$$

Proof Again, by (2.30), we have

$$U_{2m+1} = \sum_{k=0}^{m} (-1)^k \binom{2m-k}{k} P^{2m-2k} Q^k. \tag{2.64}$$

The p-adic valuation of $P^{2m-2k}Q^k$ is $2ma - (2a-b)k$, which reaches an absolute minimum when $k = m$. As, for $k = m$, the binomial coefficient

$$\binom{2m-k}{k} = 1$$

is not divisible by p, the p-adic valuation of U_n is decided by the last term of the sum in (2.64). Hence, we obtain

$$\nu_p(U_n) = 2ma - (2a-b)m = bm.$$

□

We now look at the valuation of U_{2n} when $2a > b$. We begin with a lemma established with the method and notation of Theorem 43.

Lemma 18 *If $2a = b + c$ with $b \geq 2$ even and $c \geq 0$, then*

$$U_n(P, Q) = p^{(n-1)\frac{b}{2}} \cdot U_n(p^{c/2}P', Q').$$

Proof Note that

$$P^{n-1-2k}Q^k = p^{(n-1-2k)\frac{b}{2}} (p^{c/2}P')^{n-1-2k} \cdot p^{bk} Q'^k.$$

Therefore, by (2.31), $U_n = \Psi_n(P, Q) = p^{(n-1)b/2} U_n(p^{c/2}P', Q')$. □

Theorem 45 *Suppose p is a special prime, $P = p^a P'$, $Q = p^b Q'$ with $2a > b$, and $p \nmid P'Q'$. Then, for all $n \geq 1$,*

$$\nu_p(U_{2n}) = bn + (a-b) + \nu_p(n) + h_n, \tag{2.65}$$

where

$$h_n = \nu_p(P'^2 - Q') \cdot [2 \leq p \leq 3] \cdot [2a = b+1] \cdot [p \mid n].$$

Proof By (2.20),

$$U_{2n} = U_2(P,Q)\cdot U_n(V_2,Q^2) = P\cdot U_n(V_2,Q^2). \tag{2.66}$$

Set $a' := \nu_p(V_2) = \nu_p(P^2-2Q)$ and $b' := \nu_p(Q^2) = 2b$. We see that

$$a' = \begin{cases} b, & \text{if } p \text{ is odd;} \\ b+1, & \text{if } p=2 \text{ and } 2a \geq b+2; \\ b+1+\nu_2(P'^2-Q'), & \text{if } p=2 \text{ and } 2a = b+1. \end{cases} \tag{2.67}$$

Define c' by $2a' = b' + c'$. Since $b' = 2b$ is even, we apply Lemma 18 to $U(V_2,Q^2)$ to yield

$$U_n(V_2,Q^2) = p^{(n-1)b'/2}U_n(p^{c'/2}V_2', Q'^2), \tag{2.68}$$

where $V_2' = p^{-a'}V_2$.

Case 1. $p=2$. Note that, by (2.67), $c' = 2(1+\nu'\cdot[2a=b+1])$ with $\nu' = \nu_2(P'^2-Q')$. Since $c'>0$, 2 is a regular prime of rank 2 and rank exponent $c'/2$ in $U(p^{c'/2}V_2', Q'^2)$. Thus, combining (2.66) and (2.68) with (2.59), we obtain

$$\begin{aligned} \nu_2(U_{2n}) &= \nu_2(P) + \nu_2(p^{(n-1)b'/2}) + \nu_2\big(U_n(p^{c'/2}V_2', Q'^2)\big) \\ &= a + (n-1)b + \big((c'/2-1)+\nu_2(n)\big)\cdot[2\mid n] \\ &= bn + (a-b) + \big(\nu'\cdot[2a=b+1]+\nu_2(n)\big)\cdot[2\mid n]. \end{aligned}$$

That is,

$$\nu_2(U_{2n}) = bn + (a-b) + \nu_2(n) + \nu'\cdot[2a=b+1]\cdot[2\mid n],$$

which corresponds to (2.65).

Case 2. $p\geq 3$. We see that $a' = b'/2 = b$ so that $c'=0$. Hence, by (2.68),

$$\nu_p\big(U_n(V_2,Q^2)\big) = (n-1)b + \nu_p\big(U_n(p^{-b}V_2, Q'^2)\big)$$

and, by (2.59), we get

$$\nu_p\big(U_n(V_2,Q^2)\big) = (n-1)b + \big((\nu-1)+\nu_p(n)\big)\cdot[\rho\mid n], \tag{2.69}$$

where ρ is the rank and ν the rank exponent of p in $U(p^{-b}V_2, Q'^2)$. By (2.66), $\nu_p(U_{2n}) = a + \nu_p\big(U_n(V_2,Q^2)\big)$, and we conclude that

$$\nu_p(U_{2n}) = bn + (a-b) + \big(\nu_p(n) + (\nu-1)\big)\cdot[\rho\mid n]. \tag{2.70}$$

To determine the values of ρ and ν, we compute the discriminant D' associated with $U(p^{-b}V_2, Q'^2)$. Thus,

$$D' = p^{-2b}\big((P^2 - 2Q)^2 - 4Q^2\big) = p^{-2b}(P^4 - 4P^2Q).$$

As $\nu_p(P^4) = 4a > 2a + b = \nu_p(4P^2Q)$, we see that

$$\nu_p(D') = -2b + (2a + b) = 2a - b > 0.$$

Therefore, $\rho(p) = p$. Furthermore, if $p \geq 5$ or if $p = 3$ and $2a \geq b + 2$, then $\nu = 1$ by Theorem 12. In those cases, we see that (2.70) yields what the theorem claims. It remains to prove that if $p = 3$ and $2a = b + 1$, then $\nu = 1 + \nu_3(P'^2 - Q')$. On the one hand, by (2.69), $\nu_3\big(U_3(V_2, Q^2)\big) = 2b + \nu$. On the other hand, $U_3(V_2, Q^2) = \frac{U_6(P,Q)}{U_2(P,Q)} = (P^2 - Q)(P^2 - 3Q)$. Thus,

$$\nu_3\big(U_3(V_2, Q^2)\big) = b + \big((b + 1) + \nu_3(P'^2 - Q')\big) = 2b + 1 + \nu_3(P'^2 - Q').$$

This yields the value of ν. □

We summarize the last three theorems integrating the cases when $b = 0$ into our statement and avoiding the use of Iverson symbols.

Theorem 46 *Suppose $U = U(P, Q)$, $U' = U(P', Q')$, where $P = p^a P'$, $a > 0$, $Q = p^b Q'$, $b \geq 0$, and $p \nmid P'Q'$.*
If $b \geq 2a$, then, for all $n \geq 1$,

$$\nu_p(U_n) = (n - 1)a + \nu_p(U'_n).$$

If $2a > b$, then for all $n \geq 1$,

$$\begin{aligned} \nu_p(U_{2n+1}) &= bn, \\ \nu_p(U_{2n}) &= bn + (a - b) + \nu_p(n) + h, \end{aligned}$$

where

$$h = \begin{cases} \nu_p(P'^2 - Q'), & \text{if } 2 \leq p \leq 3,\ 2a = b + 1 \text{ and } p \mid n; \\ 0, & \text{otherwise.} \end{cases}$$

Now we express the p-adic valuation of V_n. By the identity $U_{2n} = U_n V_n$, we have $\nu_p(V_n) = \nu_p(U_{2n}) - \nu_p(U_n)$. Thus, using Theorem 46, we readily obtain the following:

Theorem 47 *Suppose $V = V(P, Q)$, $V' = V(P', Q')$, where $P = p^a P'$, $a > 0$, $Q = p^b Q'$, $b \geq 0$, and $p \nmid P'Q'$. If $b \geq 2a$, then, for all $n \geq 1$,*

$$\nu_p(V_n) = na + \nu_p(V'_n).$$

If $2a > b$, then, for all positive V indices,

$$\begin{aligned} \nu_p(V_{2n+1}) &= bn + a + \nu_p(2n + 1) + k, \\ \nu_p(V_{2n}) &= bn + \ell, \end{aligned}$$

where

$$k = \begin{cases} \nu_3(P'^2 - Q'), & \text{if } p = 3,\ 2a = b+1 \text{ and } n \equiv 1 \pmod 3; \\ 0, & \text{otherwise,} \end{cases}$$

and

$$\ell = \begin{cases} 1 + \nu_2(P'^2 - Q'), & \text{if } p = 2,\ 2a = b+1 \text{ and } n \equiv 1 \pmod 2; \\ 1, & \text{if } p = 2 \text{ and } 2 \mid n \text{ or } 2a > b+1; \\ 0, & \text{otherwise.} \end{cases}$$

References

1. C. Ballot, *Lucas sequences with cyclotomic root field*, Dissertationes Math. **490** (2013), 92 pp.
2. C. Ballot, *The p-adic valuation of Lucas sequences when p is a special prime*, Fibonacci Quart. **57** (2019), 265–275.
3. R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math. (2) **15** (1913–14), no. 1-4, 30–48, 49–70.
4. F. G. Dorais and D. W. Klyve, *A Wieferich prime search up to* 6.7×10^{15}, J. Integer Seq. **14** (2011), Art. 11.9.2, 14pp.
5. A. Granville and M. Monagan, *The first case of Fermat's last theorem is true for all prime exponents up to 714,591,416,091,389*, Trans. Amer. Math. Soc. **306** (1988), no. 1, 329–359.
6. H. W. Gould, *The Girard-Waring power sum formulas for symmetric functions and Fibonacci sequences*, Fibonacci Quart. **37** (1999), 135–140.
7. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford at the Clarendon Press, London, 4th edition, 1960.
8. J. Klaška, *Donald Dines Wall's conjecture*, Fibonacci Quart. **56** (2018), 43–51.
9. J. Lagarias, *The set of primes dividing the Lucas numbers has density 2/3*, Pacific J. Math. **118**, 2 (1985), 449–461; Errata: Pacific J. Math. **162**, 2 (1994), 393–397.
10. D. H. Lehmer, *An extended theory of Lucas' functions*, Annals of Math. **31** (1930), 419–448.
11. T. Lengyel, *The order of the Fibonacci and Lucas numbers*, Fibonacci Quart. **33** (1995), 234–239.
12. É. Lucas, *Théorie des fonctions simplement périodiques*, Amer. J. Math. **1** (1878), 184–240, 289–321.
13. É. Lucas, *Théorie des Nombres*, Éditions Jacques Gabay, 1991. (Authorized re-edition of the original 1891 Gauthier-Villars edition.)
14. P. Moree, *On the divisors of* $a^k + b^k$, Acta Arith. **80** (1997), no. 3, 197–212.

15. P. Ribenboim, *The Fibonacci numbers and the Arctic Ocean*, Proceedings of the 2nd Gauss Symposium. Conference A: Mathematics and Theoretical Physics, (Munich, 1993), 41–83, Sympos. Gaussiana, de Gruyter, Berlin, 1995.
16. C. Sanna, *The p-adic valuation of Lucas sequences*, Fibonacci Quart. **54** (2016), 118–124.
17. H. C. Williams, *Édouard Lucas and Primality Testing*, Canadian Math. Soc. Series of Monographs and Advanced Texts, John Wiley and Sons, NY, 1998.

Chapter 3
Applications

I suspect at its best your education's main motive is to fuel your curiosity and teach you how to find things for yourself . . . The educationists seem to think in terms of methodical steps but a teacher brimming with passion for the subject is what actually works. (Jim Harrison in "Off to the Side")

Abstract The purpose of this chapter is to review several diverse applications of the Lucas functions, particularly in the area of computational number theory. We will begin with a largely historical description of the Mersenne primes and then examine how the Lucas functions have been applied to the problem of primality testing. As this requires that we be able to compute U_n and/or V_n for large values of n, we provide in Sect. 3.3 some algorithms by which this can be done. We next describe several subjects, such as solving congruences, integer factorization, Diophantine equations, and cryptography in which the Lucas functions have been applied.

3.1 Mersenne Primes

We have already mentioned that a very early application of the Lucas sequences was to the problem of proving that $2^{127} - 1$ is a prime. For reasons that we will discuss later in this section, it is now customary to call prime numbers of the form $2^n - 1$ Mersenne primes. In this section, we provide a brief discussion of the history and the primality of such numbers; more detail and references for this material can be found, for example, in Sects. 1.4 and 2.1 and Chap. 3 of [77].

We say that an integer d is an *aliquot* or *proper divisor* of a positive integer n if $0 < d < n$ and d divides n. For example, 3 is an aliquot divisor of 6, but neither 5 nor 6 is. We define the function $s(n)$ of a positive integer n to be the sum of all the aliquot divisors of n. Some examples are

© Springer Nature Switzerland AG 2023

C. J.-C. Ballot, H. C. Williams, *The Lucas Sequences*, CMS/CAIMS Books in Mathematics 8, https://doi.org/10.1007/978-3-031-37238-4_3

$$s(6) = 1 + 2 + 3 = 6,$$
$$s(28) = 1 + 2 + 4 + 7 + 14 = 28,$$
$$s(60) = 1 + 2 + 3 + 4 + 5 + 6 + 10 + 12 + 15 + 20 + 30 = 108.$$

Euclid defined a positive integer n to be *perfect* if $s(n) = n$. We see from the above that both 6 and 28 are perfect. It is not clear what the origin of this concept is, but it is telling that if we have $s(n) = n$, then the sum of the reciprocals of all the divisors of n is 1. As much of Greek mathematics at the time of Euclid and earlier was being developed in the Egyptian city of Alexandria, it is possible that the idea of numerical perfection arose from the ancient Egyptian technique of performing arithmetic using only unit fractions (reciprocals of positive integers).

Euclid proved that if

$$m = 2^{n-1}(2^n - 1),$$

where $2^n - 1$ is a prime, then m is perfect. Much later, Euler, in a paper published posthumously in 1849, showed that if m is an even perfect number, then it must be of Euclid's form. Although there has been much activity in searching, no odd perfect number is currently known; if one does exist, it must exceed 10^{1500} (Ochem and Rao [56]).

Thus, to find the even perfect numbers, it is necessary to find the values of n such that $2^n - 1$ is prime. As we mentioned earlier, such numbers are today called Mersenne primes after the French Minim friar Marin Mersenne (1588–1648). Mersenne was very much involved in the organization of European culture during his time; he entertained several important scientific visitors at his cell and maintained a voluminous correspondence with many of the leading savants of the seventeenth century. For much more information on these activities, especially as they affected mathematics, the reader is referred to the paper of Grosslight [28].

In 1644, Marin Mersenne stated that all the values of $n \leq 257$ for which $2^n - 1$ is prime are given in the following list:

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257.$$

(The correct list is $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$, but this was not proved until more than two centuries later.) It is because of Mersenne's early interest in numbers of the form $M_n = 2^n - 1$ that they are today called *Mersenne numbers*. We remark here that (M_n) $(= (U_n(3, 2)))$ is a divisibility sequence. It follows that if M_n is a prime, then so must n be a prime.

The early Greeks knew of the first four numbers in Mersenne's list and possibly more. At the time of this writing, 51 Mersenne primes have been identified. All of these can be found at the GIMPS [26] (Great Internet Mersenne Prime Search) website. The 51st of these is $M_{82589933}$, a number of over 24 million decimal digits and the largest prime currently known.

When Lucas published [41], he was unaware of Mersenne's list; he learned of it a few months later from Genocchi [36] and was more impressed by it than he should have been. This was because Mersenne was a correspondent of Pierre de Fermat, one of Lucas' mathematical heroes, and this to Lucas meant that Mersenne was likely in possession of unpublished and important mathematical information that had been lost.

We have already stated that Lucas made use of the properties of the Fibonacci and Lucas numbers to prove that M_{127} is a prime. The two theorems that he relied on in [41] were not proved there or correctly in any of his subsequent papers. It was Carmichael [19] in 1913 who provided correct proofs of these results. Nevertheless, it seems that Lucas had the right idea, and in a paper (Lucas [42]) that he published in April 1877, but had largely completed as early as August of 1876, he gave a reasonably complete (for Lucas) and mostly correct account of his ideas for proving M_{127} a prime. He knew that (F_n) is a divisibility sequence and that $F_{2n} = F_n L_n$, $L_{2n} = L_n^2 - 2(-1)^n$, and $L_n^2 - 5F_n^2 = 4(-1)^n$. From the last of these, he knew that $\gcd(F_n, L_n) \mid 2$. Furthermore, he was aware that for any positive m, there exists the rank of appearance $\rho(m)$ of m in (F_n) and that if $m \mid F_k$, then $\rho(m) \mid k$. He proved that if p $(\neq 5)$ is a prime and we define $\epsilon_p = 1$ when $p \equiv \pm 1 \pmod 5$ and $\epsilon_p = -1$, otherwise, then $\rho(p) \mid p - \epsilon_p$.

Now put $r_i = L_{2^i}$ and $s_i = F_{2^i}$. We have $r_1 = L_2 = 3$, $r_{i+1} = r_i^2 - 2$, and r_i is odd for $i \geq 1$. Also, $s_{i+1} = s_i r_i$ and $\gcd(s_i, r_i) = 1$. At this point, Lucas once again appeals to a result for which he did not have a correct proof, but he was likely aware that this rather general result was not needed for his immediate purposes. Let p be any odd prime such that $p \mid r_i$ (note that $p \neq 5$ because 2 is a quadratic nonresidue of 5). We see that $p \mid s_{i+1}$ and because $\gcd(s_i, r_i) = 1$, we have $p \nmid s_i$. It follows that $\rho(p) \mid 2^{i+1}$, $\rho(p) \nmid 2^i$, and therefore $\rho(p) = 2^{i+1}$. Since $\rho(p) \mid p \pm 1$, we have $2^{i+1} \mid p \pm 1$, which means that $p = 2^{i+1}k \pm 1$. Thus, Lucas could show that if $N = M_n = 2^n - 1$ and $N \mid r_i$, then any prime divisor p of N must be of the form $2^{i+1}k \pm 1$ $(\geq 2^{i+1} - 1)$. If $n \equiv 3 \pmod 4$, then $M_n = 2^{4t+3} - 1 \equiv 8 - 1 \equiv 2 \pmod 5$. Thus, if $N = M_n$ is a prime, then $\epsilon_N = -1$, and we have $N \mid F_{N+1}$. Since

$$\begin{aligned} F_{N+1} = s_n &= s_{n-1} r_{n-1} = s_{n-2} r_{n-2} r_{n-1} = s_{n-3} r_{n-3} r_{n-2} r_{n-1} \\ &= r_1 r_2 r_3 \cdots r_{n-1}, \end{aligned}$$

Lucas was aware that the values of the r_i here must be prime to one another. Thus, we can test N for primality simply by finding some i $(1 \leq i \leq n-1)$ such that $N \mid r_i$; such a value of i must exist if N is a prime. A somewhat abridged (and corrected) version of Lucas's test (Lucas [41]) is the following:

Theorem 48 *Let $N = M_n = 2^n - 1$ with $n \equiv 3 \pmod 4$. If none of the r_i for $i = 1, 2, 3, \ldots, n-1$ is divisible by N, then N is composite. If i is the least value of j $(1 \leq j \leq n-1)$ such that $N \mid r_j$, then any prime divisor p of N must be of the form $2^{i+1}k \pm 1$.*

Notice that if $2i \geq n$, then the least prime which can divide N must exceed $\sqrt{N}$, which means that N must be a prime; thus, if M_n divides r_{n-1}, then M_n is a prime. At this point (1876), Lucas was unaware that testing the divisibility of r_{n-1} by M_n is not only sufficient to prove the primality of $M_n = 2^n - 1$ with $n \equiv 3 \pmod 4$, but it is also necessary. Two years later, he showed (Lucas [45]) that if p is any prime such that $(5 \mid p) = -1$ and $p \equiv -1 \pmod 4$, then $L_{p+1} \equiv -2 \pmod p$. Hence, if $N = M_n$ is a prime, then since $M_n \equiv -1 \pmod 4$, we have $-2 \equiv L_{N+1} = L^2_{(N+1)/2} - 2$, and we get $N \mid L_{(N+1)/2}$ or $N \mid r_{n-1}$. Thus, Lucas discovered:

Theorem 49 *If $M_n = 2^n - 1$ with $n \equiv 3 \pmod 4$, then M_n is a prime if and only if M_n divides r_{n-1}, where $r_1 = 3$ and $r_{i+1} \equiv r_i^2 - 2 \pmod{M_n}$.*

This, of course, is a test for the primality of $M_n = 2^n - 1$ with $n \equiv 3 \pmod 4$, but why did he choose to test M_{127}? Had he known of Mersenne's list, this would be easier to answer, but all he knew was that $127 \equiv 3 \pmod 4$ and 127 is a prime. There are several other candidates that he might have tried, and it remains a mystery as to why he selected M_{127}. Possibly, he was impressed by the following:

$$3 = 2^2 - 1 = M_2, 7 = 2^3 - 1 = M_3, 127 = 2^7 - 1 = M_7,$$

and thought it was natural to try M_{127} as it is the next number in the progression.[†] In any event, he put $r_1 = 3$ and computed $r_{126} \pmod{M_{127}}$ recursively by using $r_{i+1} \equiv r_i^2 - 2 \pmod{M_{127}}$. This requires 125 modular squaring operations, most of which involve numbers of 39 digits, at the time an enormous undertaking. However, by observing the simple congruence

$$2^{m+n} \equiv 2^m \pmod{M_n},$$

he was able to develop an ingenious technique, involving the simple movement of pawns on a 127×127 chessboard, to compute the value of $r_{i+1} \equiv r_i^2 - 2 \pmod{M_{127}}$ from the value of $r_i \pmod{M_{127}}$. As his overall procedure was a somewhat exacting and time-consuming process, he only performed it once and at the end discovered that $r_{126} \equiv 0 \pmod{M_{127}}$.

Lucas realized that he could not use the Fibonacci and Lucas numbers to establish the primality of $M_n = 2^n - 1$ with $n \equiv 1 \pmod 4$ because in this case, $M_n \equiv 1 \pmod 5$ and therefore $\epsilon_{M_n} = 1$ whenever M_n is a prime. Perhaps this is what motivated him to investigate the features of the Lucas sequences. He quickly discovered that the properties of the Fibonacci and Lucas numbers could be extended to (U_n) and (V_n), but it took him several months to produce a prime test for such M_n. In Lucas [43], he suggests using

[†] Thus, M_{127} is a Mersenne prime, but $M_{M_{127}}$ which has more than 10^{37} digits is currently out of reach.

$P = 4$ and $Q = 1$. In this case, $D = 12$ and $(D \,|\, M_n) = (3 \,|\, M_n)$. Since $M_{2k+1} = 2^{2k+1} - 1 \equiv 1 \pmod 3$ and also $M_{2k+1} \equiv -1 \pmod 4$, we get $(3 \,|\, M_n) = -(M_n \,|\, 3) = -1$. If we put $r_i = V_{2^i}$, then $r_0 = V_1 = 4$ and $r_{i+1} = r_i^2 - 2$ for $i \geq 0$. Thus, we have $r_{n-1} = V_{(N+1)/2}$ when $N = M_n$. Proceeding in an analogous fashion to the case of $n \equiv 3 \pmod 4$, we see that if $N \mid r_{n-1}$, then N must be a prime. Notice that because we only assumed here that n is odd, this test will also work in the case that $n \equiv 3 \pmod 4$. This, of course, is half of the celebrated Lucas-Lehmer test for the primality of Mersenne numbers. Lucas, however, paid little attention to it, mentioning it as little more than an afterthought at the end of his paper, but he did cite it in Lucas [46], as this was the test used by Hudelot to ascertain the primality of M_{61}. In [45], he unwittingly proved that this test was both necessary and sufficient for any M_n to be prime for any odd n $(= 2m + 1) \geq 3$. In the last result of this paper, he puts $P = 2^{m+1}$ and $Q = -1$; then $D = 2^{2m+2} + 4 = 4(2^{2m} + 1)$. If $N = M_n$, then the Jacobi symbol

$$\begin{aligned}\epsilon_N = (D \,|\, N) &= (2^{2m} + 1 \,|\, 2^{2m+1} - 1) = (2^{2m+1} - 1 \,|\, 2^{2m} + 1) \\ &= (-3 \,|\, 2^{2m} + 1) = (2^{2m} + 1 \,|\, 3) = (2 \,|\, 3) = -1.\end{aligned}$$

Thus, by the same reasoning as used above, we see that if $N \mid V_{(N+1)/2}$, then N must be a prime. Earlier in the paper, Lucas had established that if p is an odd prime, then for any P and Q, we have

$$2V_{p+1} \equiv P^{p+1} + D^{(p+1)/2} \equiv P^2 + \epsilon_p D \pmod p.$$

Thus, if $\epsilon_p = -1 = Q$, we get $V_{p+1} \equiv -2 \pmod p$. Since $V_{p+1} = V_{(p+1)/2}^2 - 2Q^{(p+1)/2}$, it follows that $V_{(p+1)/2} \equiv 0 \pmod p$ whenever $p \equiv 3 \pmod 4$.

As a consequence of the above, we see that if $N = M_n$ is a prime, then $N \mid V_{(N+1)/2}$ when $P = 2^{m+1}$ and $Q = -1$. If, as earlier, we define $r_i = V_{2^i}$, then $r_1 = V_2 = P^2 - 2Q = 2^{2m+2} + 2 \equiv 4 \pmod N$, $r_{n-1} = V_{(N+1)/2}$, and $r_{i+1} = r_i^2 - 2$ for $i \geq 1$. Lucas had, without realizing it, proved the Lucas-Lehmer test for the primality of M_n for any odd n:

Theorem 50 *Let $N = M_n$ for any odd $n \geq 3$, and put $r_1 = 4$. If we define $r_{i+1} \equiv r_i^2 - 2 \pmod N$ for $i \geq 1$, then N is a prime if and only if $r_{n-1} \equiv 0 \pmod N$.*

This is the test that has been used to find all the known Mersenne primes M_n for $n > 127$. Indeed, it is remarkable that tests similar to this exist for more exotic forms of N. See, for instance, Roettger and Williams [61] for examples and further references.

3.2 Primality Testing

Suppose N is an odd positive integer and we wish to know whether or not N is a prime. By Fermat's little theorem, we know that if N is a prime, then for all integers a, we must have

$$a^N \equiv a \pmod{N}. \tag{3.1}$$

Thus, if this Fermat congruence does not hold for any value of a, then N cannot be a prime. Unfortunately, for primality proving, it is possible for composite integers N to satisfy this congruence for some value of a. For example, consider $a = 2$ and $N = 2701 = 37 \cdot 73$, an example known to Lucas. Hence, the direct converse of Fermat's theorem does not hold. Indeed, there exists an infinitude of composite numbers, called Carmichael numbers, for which the Fermat congruence holds for all values of a. See, for example, Sect. 3.3 of Crandall and Pomerance [21] or Sect. 15.1 of [77]. If we want to use the Fermat congruence as a prime test, we need only concern ourselves with those values of a such that $\gcd(a, N) = 1$. In this case, the Fermat congruence becomes

$$a^{N-1} \equiv 1 \pmod{N}. \tag{3.2}$$

Thus, if (3.2) does not hold for any value of a such that $\gcd(a, N) = 1$ and $1 < a < N$, then N cannot be a prime. Of course, if $\gcd(a, N) \neq 1$ and $1 < a < N$, then it is not necessary to verify (3.2) because N is clearly composite. It can also be shown that if N satisfies (3.2) for all a such that $\gcd(a, N) = 1$, then N is a Carmichael number.

Now observe that a Mersenne number is a special case of a number N for which we know all of the divisors of $N + 1$. In order to prove such values of N to be prime, Lucas [44, Sect. 27] advocated the use of what he called his *fundamental theorem*. This holds for all regular U sequences.

Theorem. If N is odd and $N \mid U_{N-\gamma}$, where $|\gamma| = 1$, but $N \nmid U_d$ for all aliquot divisors d of $N - \gamma$, then N is a prime.

Notice that, if for some integer a, we put $P = a + 1$ and $Q = a$, the above result can be used to prove the following corollary:

Corollary. If N is odd and $N \mid a^{N-1} - 1$ and $N \nmid a^d - 1$ for all aliquot divisors d of $N - 1$, then N is a prime.

This result was what Lucas [47, p. 441] considered to be the converse of Fermat's theorem. Later, Lehmer [34] pointed out that this result could be made more efficient by replacing the values of d above by $(N - 1)/p$ for each distinct prime divisor p of $N - 1$. A similar observation can also be applied to Lucas' fundamental theorem.

Although he made several attempts, Lucas was never able to provide a correct proof of his fundamental theorem; the ingredients for providing a correct proof were finally given by Carmichael [19]. A somewhat more accessible proof can be found in Sect. 4.3.

The difficulty in using Lucas' fundamental theorem in primality proving is that in almost all cases, the complete factorization of $N - \gamma$ is not available. In [44] and in some earlier papers, Lucas used his functions to test numbers other than the Mersenne numbers for primality. For example, although he did not state this result explicitly, Lucas seemed to be aware of the following theorem.

Theorem 51 *Let $N = A2^n - 1$, $n \geq 1$, where A is odd and $A < 2^n$. If $\gcd(N, Q) = 1$ and $N \mid V_{(N+1)/2}$, then N is a prime.*

Proof Suppose p is any prime divisor of N. Then $p \mid V_{(N+1)/2}$, and it follows that $p \mid U_{N+1}$. Thus, $\rho(p) \mid A2^n$. Since p does not divide Q, we see, by (2.8), that p cannot divide $U_{(N+1)/2}$ and therefore $\rho(p) \nmid A2^{n-1}$. We must have $2^n \mid \rho(p)$, which means, by the reasoning used in the proof of Theorem 48 or by appealing directly to Theorem 9, that $p = k2^n \pm 1$. If $p = 2^n - 1$, then $2^n \equiv 1 \pmod{p}$ and thus $N \equiv A - 1 \pmod{p}$. Since $A - 1 < 2^n - 1$, we find that $A = 1$, which means that $N = p$. Otherwise, $p \geq 2^n + 1 > \sqrt{N}$, which also implies the primality of N. □

He also discussed the primality of numbers of the form

$$Ap^n + \gamma, \tag{3.3}$$

where $\gamma = \pm 1$, p is a prime, and $p \nmid A$ (in Lucas' tests, $p = 2, 3, 5$, and γ is restricted to be 1 when $p = 5$). Unfortunately, his tests were given without proof and need some corrections and modifications, which were provided recently by Roettger et al. [60]. Furthermore, these tests are sufficiency tests only. A version of the test of Theorem 51 which is both necessary and sufficient was given by Lehmer [36].

Theorem 52 *Let $N = A2^n - 1$, where $n \geq 1$, A is odd, and $A < 2^n$. If $(D \mid N) = (Q \mid N) = -1$, then N is a prime if and only if $N \mid V_{(N+1)/2}$.*

Proof This result follows from the law of appearance (Theorem 9), Theorem 36, and Theorem 51. □

This result, however, is not effective in that it does not provide an explicit recipe for finding the values of P and Q which can be used. However, in the case where $3 \nmid AN$, it is a simple matter to see that when $n \geq 3$, we can always use $P = 2$ and $Q = -2$, but when $3 \mid A$, the problem of finding suitable values for P and Q becomes more difficult; however, in [12], Bosma showed how to produce such P and Q as long as $A \neq 4^m - 1$. These results were improved by Berrizbeitia and Berry [7] to the case of $5 \nmid A$. More recently, Deng and Huang [22] revisited this problem and dealt with the case of $17 \nmid A$.

We can also approach this problem by using the lemma below.

Lemma 19 *Let p be a prime such that $p \equiv -1 \pmod 4$. There exist P and Q such that $(D \mid p) = (Q \mid p) = -1$ if and only if $Q \equiv a^2 + b^2$ and $P \equiv 2a \pmod p$, where a and b are integers such that $(a^2 + b^2 \mid p) = -1$.*

Proof Suppose $Q \equiv a^2+b^2$, $P \equiv 2a \pmod p$, and $(a^2+b^2 \mid p) = -1$. We have $(Q \mid p) = -1$ and $p \nmid b$. Since $D \equiv -4b^2 \pmod p$, we have $(D \mid p) = -1$. Next, suppose that $(D \mid p) = (Q \mid p) = -1$. We have $(4Q - P^2 \mid p) = 1$; hence, there must exist some c such that $c^2 \equiv 4Q - P^2 \pmod p$, and as a consequence, we have $Q \equiv (2^{-1}P)^2 + (2^{-1}c)^2 \pmod p$; the result follows on putting $a \equiv 2^{-1}P$ and $b \equiv 2^{-1}c \pmod p$. □

We can combine Theorem 52 and Lemma 19 to produce the following test:

Theorem 53 *Let $N = A2^n - 1$, where $n > 1$, A is odd, and $A < 2^n$. Let q be a prime such that $q \equiv 1 \pmod 4$ and $(N \mid q) = -1$. If a and b are integers such that $q = a^2 + b^2$ and we put $P = 2a$ and $Q = q$, then N is a prime if and only if $N \mid V_{(N+1)/2}$.*

If the q in this theorem is small, we can find a and b by trial, but if it is large, Brillhart's [13] modification of Hermite's algorithm can be used to find them very effectively.

The main ingredient in proving the above tests is the prior determination of the forms of possible prime factors of N. Most of these results make use of techniques which show that all prime divisors of N must have a certain form, but it is sometimes possible to proceed when we know that N has at least one prime divisor of a certain form.

Lemma 20 *Suppose that N is given by (3.3), where $n \geq 1$ and $A < p^n$. If N has at least one prime divisor r of the form $kp^n + \epsilon$, where $\epsilon \in \{1, -1\}$, then N is a prime.*

Proof If N is composite, then $N = rT$, where $r = kp^n + \epsilon$, $k \geq 1$, and $T > 1$. Since $rT \equiv \gamma \pmod{p^n}$, we must have $T = hp^n + \epsilon\gamma$ and $h \geq 1$. Hence, $(kp^n + \epsilon)(hp^n + \epsilon\gamma) = Ap^n + \gamma$; it follows that

$$A = hkp^n + \epsilon(\gamma k + h) = hk(p^n - 1) + (k + \epsilon)(h + \epsilon\gamma) - \gamma.$$

Suppose p is odd. In this case, since r and T must be odd, we see that both h and k are even. Hence,

$$A \geq 4(p^n - 1) - 1 > p^n,$$

which is impossible by selection of A.

Next, suppose $p = 2$. In this case, since A must be odd, we see that h and k are of different parity, and therefore $hk \geq 2$. Thus,

$$A \geq 2(2^n - 1) - 1 = 2^{n+1} - 3 > 2^n,$$

another impossibility. Hence, N must be a prime. □

Note that if use is made of the reasoning of Robinson in Theorem 10 of [59], it is often possible to refine the above argument to increase the upper bound on A.

We can now use the Lucas sequences to establish that a number N has a prime divisor of the form $kp^n + \epsilon$, where $\epsilon \in \{1, -1\}$.

Lemma 21 *Let p be a prime and N be a positive integer such that* $\gcd(N, 2pQ) = 1$. *If for some positive integer m we have $N \mid U_{mp}$ and $N \nmid U_m$, there must exist a prime divisor of N of the form $kp^n + \epsilon$, where $\epsilon \in \{1, -1\}$ and $p^n \,||\, mp$.*

Proof Since $N \mid U_{mp}$ and $N \nmid U_m$, there must exist a prime divisor r of N such that $r^a \,||\, N$ $(a \geq 1)$ and $r^a \nmid U_m$. It follows that $\rho(r^a) \mid mp$ and $\rho(r^a) \nmid m$; hence, $p^n \mid \rho(r^a)$. Since, by Corollary 11, we have $\rho(r^a) = r^k \rho(r)$ for some $k \geq 0$ and $p \neq r$, we must have $p^n \mid \rho(r)$. By Theorem 9, we have $\rho(r) \mid r - \epsilon_r$, where $\epsilon_r = 0, 1$, or -1, so we see that $r \equiv \pm 1 \pmod{p^n}$. □

By combining the results of Lemmas 20 and 21, we get the following:

Theorem 54 *Let N be of the form (3.3), where $n \geq 1$ and $A < p^n$. If* $\gcd(N, 2Q) = 1$, *$N \mid U_{N-\gamma}$, and $N \nmid U_{(N-\gamma)/p}$, then N is a prime.*

Proof Put $m = (N - \gamma)/p$. We have $p^n \,||\, mp$, and by Lemma 21, there must exist a prime divisor of N of the form $kp^n + \epsilon$, where $\epsilon \in \{1, -1\}$. Thus, N is a prime by Lemma 20. □

Theorem 51 can be generalized to deal with numbers given by (3.3).

Theorem 55 *Let N be of the form (3.3), where $n \geq 1$ and $A < p^n$. If* $\gcd(N, 2Q) = 1$ *and $N \mid U_{N-\gamma}/U_{(N-\gamma)/p}$, then N is a prime.*

Proof In the case that $p = 2$, the proof is similar to that of Theorem 51. Suppose p is odd and $s = (p - 1)/2$; by (2.38), we have

$$U_{pr}/U_r \equiv pQ^{rs} \pmod{U_r},$$

where $r = (N - \gamma)/p$. Thus, by the conditions of the theorem, $N \nmid U_{(N-\gamma)/p}$ and $N \mid U_{N-\gamma}$. The result now follows from Theorem 54. □

Unfortunately, it is rather difficult to convert Theorems 54 or 55 into necessary and sufficient tests for the primality of N. However, results in Williams [74] can be used to prove the following $p = 3$ analogue of Theorem 53.

Theorem 56 *Let N be of the form (3.3), where $p = 3$, $n \geq 1$, and $A < 3^n$. Suppose q is a prime congruent to 1 modulo 3 such that $N^{(q-1)/3} \not\equiv 1 \pmod{q}$ and $4q = t^2 + 27u^2$, where $t \equiv 1 \pmod{3}$. If* $\gcd(N, qu) = 1$, *then N is a prime if and only if $V_{2m}(t, q) \equiv -q^m \pmod{N}$, where $m = (N - \gamma)/3$.*

A somewhat more general version of this result, proved by a different technique, was given later by Berrizbeitia and Berry [5].

A proof that for any given prime $q \equiv 1 \pmod 3$, values of t and u must always exist can be found in Sect. 6 of Chap. 9 of Ireland and Rosen [31] and in Chap. 4 of Cox [20]. Also, the value of D here is $-27u^2$ and $\epsilon_N = (D \mid N) = (-3 \mid N) = (N \mid 3) = \gamma$.

Further results for a general odd p are presented at some length in Sects. 11.3 and 16.4 of [77], and this matter is examined further in Sect. 7.4. In particular, we have a generalization of Theorem 56 in Theorem 11.3.6 of [77]. This can be converted into a necessary and sufficient test (Algorithm 11.3.7 of [77]) for the primality of N in (3.4) as long as some P and Q are given such that $(D \mid N) = \gamma$, $N \nmid U_A(P, Q)$, and a prime q ($\equiv 1 \pmod p$) can be found such that $N^{(q-1)/p} \not\equiv 1 \pmod q$.

We should point out here that Berrizbeitia et al. [6] have given a very general necessary and sufficient algorithm, not requiring Lucas functions, for proving primality of a wider class of numbers than those in (3.3), but these tests are not in general effective. However, as we have pointed out earlier, in certain cases, such as the Mersenne numbers, it is possible to use the Lucas functions to produce an effective, necessary, and sufficient test for the primality of N. For example, this is always possible for a generalization of the Mersenne numbers: $N = (p-1)p^n - 1$, when $2 \le p < 10^7$, but $p \ne 3$ (see Stein and Williams [68]). The generalization $N = 2p^n - 1$ has been discussed by Roettger and Williams [62].

We have seen that the Lucas functions can be used to produce a test for the primality of N when either $N+1$ or $N-1$ has a large prime power factor. These are examples of primality proving when a partial factorization of $N \pm 1$ is available. In 1975, Brillhart, Lehmer, and Selfridge [14] showed how to make use of the Lucas functions and partial factorizations of both $N+1$ and $N-1$ in order to establish the primality of N. These techniques are also explained in Sects. 4.1 and 4.2 of [21] and in Sects. 12.2 and 12.3 of [77] and remain to this day the best methods for primality proving as long as enough factors of $N \pm 1$ are known. Of course, this is usually not the case, and many other techniques for primality proving have been advocated since 1975; these are very ably described in [21] and from a historical perspective in [77]. Since the publication of these books, there have been several further advances. In 2002, Agrawal, Kayal, and Saxena announced a deterministic polynomial time algorithm for primality proving. Their technique, which does not involve Lucas functions, is described in [2] and in the book of Dietzfelbinger [24]. See also the insightful paper of Granville [27]. The elliptic curve primality proving (ECPP) technique of Atkin and Morain (see Chap. 7 of [21]) has been considerably refined by Morain [51], resulting in what is called fastECPP. This method has been used by Franke et al. [25] to establish the primality of numbers of up to 10 000 decimal digits.

We noted at the beginning of this section that it is possible for a composite N to satisfy (3.2) for some $a > 1$ such that $\gcd(a, N) = 1$. We call such a

value of N a *base a pseudoprime* or *a-psp*. By defining ϵ_N to be the value of the Jacobi symbol $(D \mid N)$, we can extend this idea to the Lucas function U_n. For a given pair of coprime integers P, Q, we say that N is a *Lucas pseudoprime* if N is composite, $\gcd(N, QD) = 1$, and

$$U_{N-\epsilon_N}(P, Q) \equiv 0 \pmod N.$$

Certainly, by the law of appearance, this congruence must hold when N is a prime.

Suppose, for a given odd N, we define D to be the first element in the sequence $\{5, -7, 9, -11, 13, \ldots\}$ such that $(D \mid N) = -1$. In spite of the offer of a cash reward, since 1980, no composite N has ever been found for which N is both a 2-psp and a Lucas pseudoprime with $P = 1$ and $Q = (1 - D)/4$. Undoubtedly, such N exist, but they seem to be very rare. This observation has led to the inclusion of this Lucas pseudoprime test in NIST's Federal Information Processing Standards Publication 186-4 (Appendix C.3.3) tests for the probable primality of integers employed in digital authentication algorithms. For more information concerning this topic, see Pomerance et al. [57], Sect. 3.5 of [21], and Chap. 15 of [77].

3.3 Fast Computation of U_n and $V_n \pmod m$

Let N denote any positive integer. For any integer κ, it is well known (see, e.g., Algorithm 1.2.2 of [77]) that $\kappa^m \pmod N$ can be computed in $O(\log m)$ modular multiplication operations $\pmod N$. Now consider this problem with respect to $\kappa \in \mathbb{Q}(\sqrt{d})$, where d is an integer and $\sqrt{d}$ is irrational. We note that $\kappa = (a + b\sqrt{d})/c$, where a, b, c are in $\mathbb{Z}$, and that

$$c^m \kappa^m = \frac{V_m(P, Q)}{2} + b\sqrt{d}\, U_m(P, Q),$$

where, in this case, $P = 2a$ and $Q = a^2 - db^2$. If $\gcd(c, N) = 1$, then

$$\kappa^m \equiv V_m(P, Q)/2 + b\sqrt{d}\, U_m(P, Q) \pmod N,$$

where $P \equiv 2ac^{-1}$, $Q \equiv (a^2 - db^2)c^{-2} \pmod N$, and $cc^{-1} \equiv 1 \pmod N$. Thus, the Lucas functions can play a role in determining $\kappa^m \pmod N$. In many applications of the Lucas functions, such as primality testing, it is often necessary to compute rapidly some remote values of V_m and/or $U_m \pmod N$. As pointed out in Sect. 4.3 of [77], this can be done by first observing the simple identities:

$$\begin{aligned} U_{2n} &= 2U_{n+1}U_n - PU_n^2, \\ U_{2n+1} &= U_{n+1}^2 - QU_n^2, \\ U_{2n+2} &= PU_{n+1}^2 - 2QU_nU_{n+1}. \end{aligned} \tag{3.4}$$

We next define $\{A, B\} \equiv \{E, F\} \pmod N$ to mean that $A \equiv E$ and $B \equiv F \pmod N$. Let $(b_0, b_1, b_2, \ldots, b_k)_2$ be the binary representation of m. Suppose $\mathcal{P}_i = \{A, B\}$; when $b_{i+1} = 0$, put $\mathcal{P}_{i+1} \equiv \{2AB - PA^2, B^2 - QA^2\} \pmod N$; when $b_{i+1} = 1$, put $\mathcal{P}_{i+1} \equiv \{B^2 - QA^2, PB^2 - 2QAB\} \pmod N$. If we put $\mathcal{P}_0 \equiv \{1, P\}$, we see by the identities (3.4) that $\mathcal{P}_k \equiv \{U_m, U_{m+1}\}$. We can find $V_m \pmod N$ by using the identity $V_m = 2U_{m+1} - PU_m$.

The above technique can be somewhat less efficient than the following method, which can be used when $\gcd(PQD, N) = 1$, a case that occurs frequently. We define

$$W_n \equiv Q^{-n}V_{2n} \pmod N, \tag{3.5}$$

where $QQ^{-1} \equiv 1 \pmod N$ and $Q^{-n} = (Q^{-1})^n$. Also, for any integers s and t, we have $W_{2s} \equiv W_s^2 - 2 \pmod N$ by (2.24) and $W_{s+t} \equiv W_sW_t - W_{s-t} \pmod N$ by (2.17). We also have the following results, all modulo N:

$$\begin{aligned} V_{2h} &\equiv Q^hW_h, \\ PV_{2h+1} &\equiv Q^{h+1}(W_h + W_{h+1}), \\ DU_{2h+1} &\equiv Q^{h+1}(W_{h+1} - W_h), \\ PDU_{2h} &\equiv Q^h(2QW_{h+1} - (P^2 - 2Q)W_h). \end{aligned} \tag{3.6}$$

Thus, if $h = \lfloor m/2 \rfloor$, we can compute V_m and U_m modulo N if we know W_h and $W_{h+1} \pmod N$. Now suppose that $(b_0, b_1, b_2, \ldots, b_k)_2$ is the binary representation of h, and put $\mathcal{P}_0 \equiv \{W_1, W_2\}$, where $W_1 \equiv P^2Q^{-1} - 2 \pmod N$ and $W_2 \equiv W_1^2 - 2 \pmod N$. Suppose $\mathcal{P}_i = \{A, B\}$; if $b_{i+1} = 0$, put $\mathcal{P}_{i+1} \equiv \{A^2 - 2, AB - W_1\}$; if $b_{i+1} = 1$, put $\mathcal{P}_{i+1} \equiv \{AB - W_1, B^2 - 2\} \pmod N$. We see that $\mathcal{P}_k \equiv \{W_h, W_{h+1}\}$.

Furthermore, given values for W_h and $W_{h+1} \pmod N$ and some positive integer t, we can quickly evaluate $W_{th} \pmod N$. If $(b_0, b_1, b_2, \ldots, b_k)_2$ is the binary representation of t and $\mathcal{P}_0 \equiv \{W_h, W_{h+1}\}$, we compute $\mathcal{P}_k \equiv \{W_{th}, W_{t(h+1)}\}$ in a similar fashion to the above scheme. For $\mathcal{P}_i = \{A, B\}$, we calculate $\mathcal{P}_{i+1} \equiv \{A^2 - 2, AB - W_h\} \pmod N$ when $b_{i+1} = 0$; if $b_{i+1} = 1$, compute $\mathcal{P}_{i+1} \equiv \{AB - W_h, B^2 - 2\} \pmod N$.

We next define the polynomial $G_m(x)$ for $m \geq -1$ by $G_{-1}(x) = -1$, $G_0(x) = 1$, and $G_{k+1}(x) = xG_k(x) - G_{k-1}(x)$ $(k = 0, 1, 2, \ldots)$. This polynomial is related to the $\psi_n(x)$ polynomial of Sylvester [71, p. 366ff]; more information can be found concerning it in Sect. 4.2. It is easy to establish by induction that

$$(y^{2m+1} - 1)/(y - 1) = y^mG_m(y + y^{-1}) (m \geq -1).$$

Note that this holds even when $y = 1$ because $G_m(2) = 2m + 1$. We also have $G_m(-2) = (-1)^m$ for any m and $G_m(-1) = 1$ whenever $3 \mid m$. If we put $r = 2s + 1$ and $y = -(\alpha/\beta)^n$, we get

$$V_{nr} = (-1)^s Q^{ns} G_s(-V_{2n}/Q^n) V_n \equiv (-1)^s Q^{ns} G_s(-W_n) V_n \pmod{N}; \tag{3.7}$$

if we put $y = (\alpha/\beta)^n$, we get

$$U_{nr} = Q^{ns} G_s(V_{2n}/Q^n) U_n \equiv Q^{ns} G_s(W_n) U_n \pmod{N}. \tag{3.8}$$

If we refer back to Theorem 55 and put $m = (N - \gamma)/r$, we see by (3.8) that $N \mid U_{N-\gamma}/U_{(N-\gamma)/r}$ if and only if $N \mid G_s(W_m)$. In the case of p odd, we can now restate Theorem 55.

Theorem 57 *Let N be of the form (3.3), where $n > 1$ and $A < p^n$. If $\gcd(N, 2Q) = 1$, $m = (N - \gamma)/p$, and $N \mid G_s(W_m)$, where $s = (p-1)/2$, then N is a prime.*

3.4 Solving Quadratic and Cubic Congruences

Let $f(x)$ be any polynomial with integer coefficients, and let m be any positive integer. There is a simple algorithm for solving

$$f(x) \equiv 0 \pmod{m};$$

simply try all possible values of x in the range $0, 1, 2, \ldots, m - 1$, and record those values which satisfy the congruence. However, this procedure, while perfectly valid, is very inefficient when m is large. More effective techniques can be found in any elementary number theory textbook, but these rely upon the ease with which m can be factored (see Sect. 3.5) and the available routines for solving

$$f(x) \equiv 0 \pmod{p},$$

where p is a prime divisor of m. The general problem of solving a polynomial congruence modulo a prime has attracted a considerable body of literature. See, for example, paragraph 4.3 of Lidl and Niederreiter [40]. In this section, we will confine our discussion of this problem to that of solving polynomial congruences of degrees 2 and 3.

We first describe how a Lucas function can be employed to solve the congruence

$$x^2 \equiv a \pmod{p}, \tag{3.9}$$

where p is an odd prime and a is a quadratic residue of p, i.e., the Legendre symbol $(a \,|\, p) = 1$. See [75, p. 228]. Put $Q = a$, and find by trial a value of P such that $(D \,|\, p) = -1$, where $D = P^2 - 4Q$. This latter process might be

considered a defect in the method, as it is unknown how many possible values of P we would have to try until we find one such that $(D \mid p) = -1$, but in practice, a suitable value for P appears after only a few trials. By Theorem 36, we must have $p \mid U_{(p+1)/2}$. Thus, by (2.8), we get $V^2_{(p+1)/2} \equiv 4Q^{(p+1)/2} \pmod{p}$. Since $Q^{(p+1)/2} = aa^{(p-1)/2} \equiv a \pmod{p}$, we see that the roots of (3.9) are given by $\pm 2^{-1} V_{(p+1)/2} \pmod{p}$.

The above idea was first suggested by Cipolla in 1903 and rediscovered by Lehmer in 1969.

We note that simpler solutions to (3.9) exist for $p = 4n+3$ and $p = 8n+5$. If $p = 4n + 3$, then

$$a^{2n+2} = aa^{2n+1} = aa^{\frac{p-1}{2}} \equiv a \pmod{p}.$$

Thus, $\pm a^{n+1} \pmod{p}$ are the solutions of (3.9).

Legendre noticed that if $p = 8n + 5$, we have

$$1 = (a \mid p) \equiv a^{\frac{p-1}{2}} = a^{4n+2} \pmod{p};$$

thus, $a^{2n+1} \equiv \pm 1 \pmod{p}$. In the case of $a^{2n+1} \equiv 1 \pmod{p}$, the solutions of (3.9) are clearly $\pm a^{n+1} \pmod{p}$; in the case of $a^{2n+1} \equiv -1 \pmod{p}$, the solutions are $\pm(1/2)(4a)^{n+1}$ because

$$\left(\pm (1/2)(4a)^{n+1} \right)^2 = 4^{2n+1} a^{2n+2} = 2^{4n+2} a^{2n+1} a \equiv -(2 \mid p) a \equiv a \pmod{p}.$$

This observation of Legendre was extended to $p = 8n + 1$ by Tonelli in 1891. Tonelli's technique was rediscovered and generalized by Shanks in 1972.

We illustrate the Cipolla-Lehmer method for a prime of the form $8n + 1$, namely, 89, and $a = 2$. Thus, $Q = 2$ and $D = P^2 - 8$. Trying $P = 1$ yields $D = -7$ and

$$(-7 \mid 89) = (89 \mid 7) = (5 \mid 7) = (2 \mid 5) = -1.$$

We need to compute V_{45}. Using a variation on what we did in the previous section, i.e., the doubling and side-step formulas $U_{2n} = U_n V_n$, $V_{2n} = V_n^2 - 2Q^n$, $U_{2n+1} = \frac{1}{2}(PU_{2n} + V_{2n})$, and $V_{2n+1} = \frac{1}{2}(DU_{2n} + PV_{2n})$, we obtain $V_{2n} = V_n^2 - 2^{n+1}$, $U_{2n+1} = \frac{1}{2}(U_{2n} + V_{2n})$, $V_{2n+1} = \frac{1}{2}(V_{2n} - 7U_{2n})$, and

n	U_n	V_n
5	−1	11
10	−11	57
11	23	67
22	28	37
44	57	32
45	0	39

so that the solutions are

$$\pm\frac{39}{2} \equiv \pm\frac{39-89}{2} \equiv \pm 25 \pmod{89}.$$

(We see that 2 is a fourth power residue modulo 89.)

For more information and references concerning the solution of the quadratic congruence, see Müller [53].

We now turn to the problem of solving the cubic congruence

$$f(x) = x^3 + ax^2 + bx + c \equiv 0 \pmod{p}, \tag{3.10}$$

where a, b, and c are integers and p (> 3) is a prime. It may seem surprising, but by using an old idea of Cailler [18], Lucas functions can be used in many cases to solve (3.10). It is well known that if we put $y = a+3x$, then $27f(x) = g(y)$, where $g(y) = y^3 - 3Ay + G$, $A = a^2 - 3b$, and $G = 2a^3 - 9ab + 27c$. Thus, any solution y of

$$g(y) = y^3 - 3Ay + G \equiv 0 \pmod{p} \tag{3.11}$$

can be readily converted to a solution x of (3.10).

If $p \mid A$, we are left with the problem of solving

$$y^3 \equiv -G \pmod{p}. \tag{3.12}$$

If $p \equiv 2 \pmod 3$, then (3.12) has the solution $y \equiv -G^{(2p-1)/3} \pmod p$. If $p \equiv 1 \pmod 3$, a necessary condition for (3.12) to have a solution is that $(-G)^{(p-1)/3} = G^{(p-1)/3} \equiv 1 \pmod p$. Put $t = (p-1)/3$, and suppose that $3 \nmid t$ (this certainly occurs when $9 \nmid p-1$). In this case, there must exist some $c \in \{1, 2\}$ such that $3 \mid ct+1$, and it is easy to see that (3.12) has the solution $y \equiv -G^{(ct+1)/3} \pmod p$. In what follows, we will extend these ideas to the case where $p \nmid A$.

We first observe that if $p \mid G^2 - 4A^3$, then it is easy to see that $y \equiv G(2A)^{-1} \pmod p$ is a solution of $g(y) \equiv 0 \pmod p$; thus, we will assume that $p \nmid G^2 - 4A^3$. It is convenient at this point to make use of the properties of finite fields; let $\mathbb{F}_p$ be the finite field containing p elements, and let $\mathbb{K}$ containing $\mathbb{F}_p$ be the finite field containing p^2 elements. We may suppose that A and $G^2 - 4A^3$ are both nonzero in $\mathbb{K}$. Also, there must exist α and β in $\mathbb{K}$ such that $\alpha + \beta = G/A$ and $\alpha\beta = A$. We have $A^2(\alpha - \beta)^2 = G^2 - 4A^3$, which means that $\alpha \neq \beta$. Now let $z = (y - \alpha)/(y - \beta) \neq 1$, where $y \in \mathbb{F}_p$ and $g(y) \equiv 0 \pmod p$; we have $y = (\beta z - \alpha)/(z - 1)$ and $g(y) = h(z)/(z - 1)^3$, where $h(z) = \beta(\alpha - \beta)^2 z^3 - \alpha(\alpha - \beta)^2$. It follows that $\beta z^3 = \alpha$ in $\mathbb{K}$. Put $D = (\alpha - \beta)^2$ and $\epsilon_p = (D \mid p)$. Since, in $\mathbb{K}$, $\alpha^p = \alpha$ when $\epsilon_p = 1$ and $\alpha^p = \beta$ when $\epsilon_p = -1$, we see that $z^{p-\epsilon_p} = 1$ in $\mathbb{K}$.

Suppose that $3 \nmid p - \epsilon_p$; then, as above, there must exist $c \in \{1, 2\}$ such that $3 \mid c(p - \epsilon_p) + 1$. Since $z^3 = \alpha/\beta$, we must have $z = (\alpha/\beta)^m$,

where $m = (c(p-\epsilon_p)+1)/3$. Since $y = (\beta z - \alpha)/(z-1)$, we see that $y \equiv QU_{m-1}(P,Q)U_m(P,Q)^{-1} \pmod{p}$ is a solution of (3.11) , where $P \equiv GA^{-1} \pmod{p}$ and $Q = A$.

Next, suppose that $3 \mid p - \epsilon_p$. In this case, since $z^{p-\epsilon_p} = 1$, we must have $(\alpha/\beta)^{(p-\epsilon_p)/3} = 1$, which is equivalent to $U_{(p-\epsilon_p)/3}(P,Q) \equiv 0 \pmod{p}$. If this latter congruence does not hold, then (3.11) has no solution. If it does hold, then put $t = (p-\epsilon_p)/3$, and suppose that $3 \nmid t$; there must exist $c \in \{1,2\}$ such that $3 \mid ct+1$ and $z = (\alpha/\beta)^m$ satisfies $z^3 = \alpha/\beta$ when $m = (ct+1)/3$; thus, as we reasoned earlier, $y \equiv QU_{m-1}(P,Q)U_m(P,Q)^{-1} \pmod{p}$ is a solution of (3.11). Hence, we can use the Lucas functions to solve (3.11) as long as $9 \nmid p - \epsilon_p$.

By using a method of Williams [76], we can also use Lucas functions to solve (3.11) without needing to compute $U_m(P,Q)^{-1} \pmod{p}$. In order to do this, we need a preliminary lemma. As earlier, we assume that $P \equiv GA^{-1} \pmod{p}$, $Q = A$, $D = P^2 - 4Q$, $\epsilon_p = (D \mid p) \neq 0$, $\eta = (Q \mid p)$, and $c \in \{1,2\}$.

Lemma 22 *If t is any divisor of $p - \epsilon_p$ such that $r = (p-\epsilon_p)/t$ is odd, then $U_{ct} \equiv 0 \pmod{p} \iff V_{ct} \equiv 2\eta^c Q^{ct/2} \pmod{p}$.*

Proof We first observe that since r is odd, we must have t even. By (2.8), it is clear that $p \mid U_{ct}$ when $V_{ct} \equiv 2\eta^c Q^{ct/2} \pmod{p}$. If $p \mid U_{ct}$, we have $p \mid U_t$ or, possibly in the case of $c = 2$ and $\eta = -1$, $p \mid V_t$ by Theorem 36. In this latter case, $V_{2t} \equiv -2Q^t \pmod{p}$. By (3.8) and the law of appearance, we get

$$0 \equiv U_{p-\epsilon_p} \equiv Q^{ts} G_s(V_{2t}/Q^t) U_t \equiv (-1)^s Q^{ts} U_t \pmod{p},$$

where $s = (r-1)/2$. Hence, we get $U_t \equiv V_t \equiv 0 \pmod{p}$, which is impossible by (2.8); thus, we can only have $p \mid U_t$ and by (2.8) $V_t \equiv 2\theta Q^{t/2} \pmod{p}$, where $\theta = \pm 1$. It follows that $V_{2t} = V_t^2 - 2Q^t \equiv 2Q^t \pmod{p}$. By (3.7), we have

$$2Q^{(p-\epsilon_p)/2} \equiv V_{p-\epsilon_p} = V_{rt} = (-1)^s Q^{ts} G_s(-V_{2t}/Q^t) V_t \equiv 2\theta Q^{rt/2}.$$

Hence, we must have $\theta = \eta$, and we have the lemma. □

We are now able to prove the following theorem.

Theorem 58 *Let p, ϵ_p, t, and r be defined as in Lemma 22, and suppose that $3 \nmid t$. Let $c \in \{1,2\}$ be such that $3 \mid ct+1$. If $p \mid U_{ct}$, then $y \equiv -\eta^c P^{-1} Q(W_{k+1} + W_k) \pmod{p}$ is a solution of (3.11), where $k = (ct-2)/6$ and W_k was defined in (3.5).*

Proof By Lemma 22, we must have $V_{ct} \equiv 2\eta^c Q^{ct/2} \pmod{p}$. By (2.11), we have

$$2V_{ct+1} = V_{ct}V_1 + DU_{ct}U_1 \equiv 2\eta^c Q^{ct/2} P \pmod{p}.$$

Hence, if $m = (ct+1)/3$, we get $V_{3m} \equiv \eta^c P Q^{ct/2} \pmod{p}$ and

$$V_m^3 - 3Q^m V_m = V_{3m} \equiv \eta^c P Q^{ct/2} \pmod{p}.$$

Since m is odd, we have $m = 2k + 1$ and $k = (ct - 2)/6$. We find that

$$(V_m Q^{-k})^3 - 3Q(V_m Q^{-k}) \equiv \eta^c PQ \pmod{p}$$

or

$$(-\eta^c V_m Q^{-k})^3 - 3A(-\eta^c V_m Q^{-k}) + G \equiv 0 \pmod{p}.$$

By the second formula in (3.6), we see that $y \equiv -\eta^c P^{-1} Q(W_{k+1} + W_k) \pmod{p}$ is a solution of (3.11). □

Thus, if $p - \epsilon_p \not\equiv 0 \pmod{9}$, we can always find a solution of (3.10) by using Lucas functions. More results, particularly for the case that $9 \mid p - \epsilon_p$, and additional references concerning solving the cubic congruence can be found in Müller [54].

Example 59 Find a solution of

$$y^3 - 21y - 7 \equiv 0 \pmod{41}. \tag{3.13}$$

In this case, we have $p = 41$, $P \equiv -1$, $Q \equiv 7$, and $D \equiv -27 \pmod{41}$. Thus, $\eta = (7 \mid 41) = -1$, $\epsilon_p = (-3 \mid 41) = -1$, and $41 - \epsilon_p = 42$. Since $3 \mid 42$ and $9 \nmid 42$, we can put $t = 42/3 = 14$ and $c = 1$ so that $m = (ct + 1)/3 = 5$ and $k = 2$. We have $U_0 = 0$, $U_1 = 1$, $U_2 = -1$, $U_3 = -6$, $U_4 = 13$, and $U_5 = 29$. Hence, $y \equiv 7 \cdot 13 \cdot 29^{-1} \equiv 7 \cdot 13 \cdot 17 \equiv 30 \pmod{41}$ is a solution of (3.13). By results in Sect. 3.3, we also have $W_1 \equiv P^2 Q^{-1} - 2 \equiv 7^{-1} - 2 \equiv 4 \pmod{41}$, $W_2 \equiv W_1^2 - 2 \equiv 14 \pmod{41}$, and $W_3 \equiv W_1 W_2 - W_1 \equiv 11 \pmod{41}$. Thus, $y \equiv -\eta^c P^{-1} Q(W_{k+1} + W_k) \pmod{41} \equiv -1 \cdot 7(14 + 11) \equiv 30$ is, as we have already seen, a solution of (3.13). □

3.5 Integer Factoring

The integer factoring problem can be stated as follows: Given an integer $N > 1$, where N is not a prime, find an integer a with $1 < a < N$ such that a is a divisor of N. This rather simple sounding request has turned out to be an enormous challenge to mathematicians since antiquity, but within the last 50 years, it has become of great importance to the problem of providing secure communication. In this section, we will only discuss the application of the Lucas functions to this problem, but there is much more to integer factorization than what we will discuss here. For further information, the reader is referred, for the early history of the problem, to Williams and Shallit [79] or various chapters of [77] and for modern techniques to [21], Lenstra [38], and Wagstaff [72].

In 1974, Pollard [58] produced a rather novel approach to this problem. He assumed that N has a prime divisor p, where the largest prime power divisor of $p-1$ is less than or equal to a preassigned bound B. Let $\mathcal{P}$ denote the set of all primes, and for each $q \in \mathcal{P}$, define the nonnegative integer $\lambda(q)$ by

$$q^{\lambda(q)} \le B < q^{\lambda(q)+1}.$$

Let R be the product of all $q^{\lambda(q)}$ for $q \in \mathcal{P}$; this is a finite product because $\lambda(q) = 0$ when $q > B$. Also, $p-1$ must be a divisor of R by our assumption. Since $a^{p-1} \equiv 1 \pmod{p}$ for any a such that $\gcd(a, N) = 1$, we must have $a^R \equiv 1 \pmod{p}$, and we find that p must be a divisor of $\gcd(a^R - 1, N)$. For any a such that $\gcd(a, N) = 1$, it is relatively easy to compute $a^R \pmod{N}$; thus, we can use the above observation to find a factor $\gcd(a^R - 1, N)$ of N, as long as our initial assumption holds. Pollard also discussed a very useful second stage of his algorithm to be used when $p-1$ has a single prime divisor r, where $r < B'$, a larger bound than B, the upper bound on all the other prime power divisors of $p-1$. It was by making use of Pollard's idea with $B = 6 \cdot 10^5$ and $B' = 10^7$ that Baillie (unpublished) discovered a new prime divisor of M_{257} in 1980. (See Sect. IIIB2 of Brillhart et al. [15].)

Guy [29] mentioned a possible technique, using Lucas functions, for factoring N when $p+1$ has only small prime power factors. This was implemented later by Williams [75]. In this algorithm, we assume that the largest prime power divisor of $p+1$, where p is some prime divisor of N, is less or equal to a preassigned bound B and, as above, let R be the product of all $q^{\lambda(q)}$ for $q \in \mathcal{P}$. In this case, we see that $p+1$ must be a divisor of R. If $\gcd(Q, N) = 1$ and $(D \,|\, p) = -1$, then $p \mid U_{p+1}(P, Q)$ by the law of appearance. Hence, as above, we find that $p \mid U_R(P, Q)$ and therefore $p \mid \gcd(U_R(P, Q), N)$. As it is more convenient to compute $W_R(P, Q)$ instead of $U_R(P, Q)$, we observe that if $p \mid U_R(P, Q)$, then $V_R^2(P, Q) \equiv 4Q^R \pmod{p}$ by (2.8) and therefore $W_R(P, Q) \equiv 2 \pmod{p}$ by (2.25). Thus, to find a non-trivial factor of N, we make use of the techniques described in Sect. 3.3 to calculate $W_R(P, Q) \pmod{N}$ and then evaluate $\gcd(W_R(P, Q) - 2, N)$. Just as in the case of Pollard's $p-1$ method, there is a second stage of the $p+1$ method. This can be used when $p+1$ has a single prime divisor r, where $r < B'$ and B' is a larger bound than B. These methods were improved later by Montgomery [50].

Bach and Shallit [3] have extended the $p-1$ and $p+1$ methods to produce a factoring technique which operates under the assumption that $\Phi_k(p)$ has only small prime power divisors. Here, $\Phi_k(x)$ denotes the kth cyclotomic polynomial, an irreducible (over the rational numbers) polynomial, of degree $\varphi(k)$, divisor of $x^k - 1$. For example, $\Phi_1(p) = p - 1$, $\Phi_2(p) = p + 1$, $\Phi_3(p) = p^2 + p + 1$, $\Phi_4(p) = p^2 + 1$, etc. See Sect. 4.3 for more information concerning the cyclotomic polynomials.

3.6 Diophantine Equations

A Diophantine equation is an indeterminate equation whose unknowns are constrained to assume integral (or rational) values. For example, an integral solution of the Diophantine equation $x^2 + y^2 = z^2$ is $(3, 4, 5)$. The study of these equations began in antiquity and continues to be an active area of research to this day. While it may appear that these objects are of little importance, they have nevertheless inspired a great deal of very fundamental mathematics; the search for all of the solutions of the Fermat Diophantine equation $x^n + y^n = z^n$ $(n > 2)$ was responsible for the development of very sophisticated results involving algebraic geometry, and attempts to solve the equations like $x^3 - 2y^3 = n$ (for a given n) stimulated much research on rational approximations to irrational numbers. For a compendium of results on this topic up to 1920, the reader is referred to the second volume of Dickson [23]; for more modern results and techniques, see Mordell [52], Schmidt [65], Shorey and Tijdeman [63], Smart [66], and Steuding [69].

One of the most studied Diophantine equations is the so-called Pell equation. This is the equation

$$x^2 - dy^2 = 1, \tag{3.14}$$

where d is a given non-square positive integer. It is important to realize that non-trivial $(y \neq 0)$ solutions always exist for (3.14), although it is not immediately clear that this is so. For example, $x^2 - 19y^2 = 1$ has the solution $(170, 39)$, but the smallest value of $|y|$ such that $x^2 - 1621y^2 = 1$ is a number of 74 decimal digits. The Pell equation often turns up in the investigation of other Diophantine equations such as $x^3 + y^3 + z^3 = 1$ (Lehmer [37]) or $(x^2 + a)(y^2 + a) = (az^2 + b^2)^2$ (Williams [73]). See also Chap. 8 of [52]. A very readable account of the Pell equation can be found in Barbeau [4].

It is well known that all solutions of (3.14) are given by (X_n, Y_n), where X_n and Y_n are generated from a fundamental solution (X_1, Y_1) by

$$X_n + \sqrt{d}\, Y_n = (X_1 + \sqrt{d}\, Y_1)^n$$

for all integral values of n. The problem of how to compute this fundamental solution is discussed in some detail in Jacobson and Williams [32]. If, as noted by Lehmer [35], we put $P = 2X_1$ and $Q = 1$, we find that $D = 4dY_1^2$ and

$$2X_n = V_n(P, Q), \quad Y_n = Y_1\, U_n(P, Q).$$

Thus, we can determine the properties of the solutions of (3.14) from the properties of the Lucas functions. Also, wherever it is possible to use the Pell equation to solve a given Diophantine equation, we will very likely need to appeal to the properties of the Lucas functions. As a simple example, suppose we wish to find a solution of the Pell equation

$$x^2 - 931y^2 = 1. \tag{3.15}$$

We observe that $931 = 7^2 \cdot 19$; since the minimal solution of $x^2 - 931y^2 = 1$ is $(170, 39)$, we need to find a value of n such that $7 \mid U_n(340, 1)$. Since $\epsilon_7 = (D \mid 7) = (19 \mid 7) = -1$ and $(Q \mid 7) = 1$, we see by the law of appearance and Theorem 36 that $n = (7 - \epsilon_7)/2 = 4$ will work and $x = V_4(340, 1)/2 = 6681448801$ and $y = 39U_4(340, 1)/7 = 218975640$ are solutions of (3.15). The theory of the Pell equation has attracted a great deal of literature, much of which is cited in [32] and Lenstra [39], to which the interested reader is referred.

The Lucas sequences have also appeared as the subject of Diophantine analysis; for example, consider the problem of finding all the Fibonacci numbers that are perfect integral squares. Credit is usually given to J. H. E. Cohn for first proving in 1964 that $F_1 = F_2 = 1$ and $F_{12} = 144$ are the only square Fibonacci numbers. However, Wilhelm Ljunggren had solved the problem more than a decade earlier, using much more sophisticated and general methods. Unfortunately, although he published his papers in English, they appeared in Norwegian venues during and around World War II and were not as well known as they should have been. More recently, the problem of finding all F_n (and L_n) which are perfect integral powers has been solved by Bugeaud, Mignotte, and Siksek [17] using very deep and powerful techniques. (The only additional numbers are $F_6 = 8$, $L_1 = 1$, and $L_3 = 4$.) The paper [17] also has extensive bibliography which we recommend to the interested reader.

3.7 Cryptography

Cryptography is the practice of designing and analyzing techniques that assure secure communication in the presence of malicious adversaries. In the last 50 years, cryptography has been the object of considerable (unclassified) research by mathematicians, computer scientists, and electrical engineers. For an overview of this subject, the reader is advised to consult any number of introductory textbooks; in particular, we suggest the books of Buchmann [16] and Stinson [70]. Also, for a more detailed treatment, the comprehensive handbook of Menezes et al. [49] is highly recommended. As both [70] and [49] contain extensive bibliographies, we will refrain from including a lot of references in this section.

Since the inception of the Internet, it has become customary to make use of public-key (or two-key) cryptography for securing Internet commerce. In such a scheme, each member of a group of individuals wishing to exchange information will have both a private key and a public key unique to that person. If Alice and Bob are members of such a group and Alice wishes to communicate with Bob, she looks up his encryption key in a public directory and encrypts her message M to him using this key. On receipt of this ciphertext, Bob uses his decryption key to decipher it and produce M. As

an example of such a cryptosystem, consider the so-called RSA system. Each member of the group, say Bob (or a trusted authority acting on Bob's behalf), selects two large primes p and q of k digits at random, keeps them secret, and computes $N = pq$. He also selects at random an integer e $(< N)$ such that $\gcd(e, \varphi(N)) = 1$ $(\varphi(N) = (p-1)(q-1))$ and solves the linear congruence

$$ed \equiv 1 \pmod{\varphi(N)}$$

by the extended Euclidean algorithm to find d with $0 < d < \varphi(N)$. Bob's public encryption key is the pair (e, N), and his private decryption key is d. If Alice wishes to send a secure, numerically encoded message M $(0 < M < N, \gcd(M, N) = 1)$ to Bob, she computes $C \equiv M^e \pmod{N}$ $(0 < C < N)$ and sends C to Bob. Bob can recover M from C by calculating

$$C^d \equiv M^{ed} \equiv M^{1+t\varphi(N)} \equiv M \pmod{N},$$

by Euler's theorem. Since $M < N$, it is uniquely determined. This scheme has been the subject of many cryptographic attacks, but with some modifications, it has withstood them all and is still widely used today. See Boneh [10].

Of course, if an adversary can factor the RSA modulus N, then he can break the system. However, in spite of the many improvements to integer factoring algorithms since the announcement of the RSA system in 1977, factoring N when $k = 1024$, say, seems still to lie in the distant future. Of course, this statement could become invalid, should some group of clever individuals develop a new and better factoring algorithm or produce a universal quantum computer with a sufficient number of qubits. At this point, the latter scenario seems more likely. For information concerning quantum computers and computing, see Kaye et al. [33].

One of the problems associated with the RSA cryptosystem is the process of selecting p and q. We note that because of the existence of the $p-1$ and $p+1$ factoring techniques, it is essential for the security of the system that each of the four numbers $p \pm 1$ and $q \pm 1$ has at least one large prime factor. The problem of producing such p and q was first examined by Williams and Schmid [78], where the use of the primality tests of [14] was advocated. Since then, there have been further developments by Shawe-Taylor [64] and Maurer [48]. This latter paper is a particularly valuable contribution to this problem.

In 1993, Smith [67] produced a public-key cryptosystem, called LUC, which was based on Lucas functions. "The basic idea behind LUC is that of providing an alternative to RSA by substituting the calculation of Lucas functions for that of exponentiation. While Lucas functions are somewhat more complex mathematically than exponentiation, they produce superior ciphers." Nevertheless, the system has some important weaknesses as pointed out by Bleichenbacher et al. [8]. However, it has since been recommended as a possible authentication system and continues to be the object of active research. (See, e.g., Ibrahimpašić [30].) If we suppose that N is an RSA

modulus and $\gcd(QD, N) = 1$, the basic idea behind LUC is the simple result, easily proved from the law of appearance, that $U_{m\psi(N)}(P, Q) \equiv 0 \pmod{N}$ and $V_{m\psi(N)}(P, Q) \equiv 2 \pmod{N}$, where m is any positive integer and $\psi(N) = (p^2 - 1)(q^2 - 1)$. In this scheme, Bob computes $\psi(N)$ and finds some positive $e < N$ at random such that $\gcd(e, \psi(N)) = 1$. As in RSA, the pair (e, N) will constitute his public key. He next solves the linear congruence

$$ed \equiv 1 \pmod{\psi(N)}$$

for his private key d. (This is not exactly what is recommended in [67], but as mentioned in [8], it avoids the problem of message dependence.)

For Alice to send a message M $(< N)$ to Bob, she first puts $P = M$ and $Q = 1$ and computes $C \equiv V_e(M, 1) \pmod{N}$ and sends C to Bob. Bob can recover M by computing $V_d(C, 1) \equiv M \pmod{N}$. To see why this works, we observe that

$$V_d(C, 1) \equiv V_d(V_e(M, 1), 1) \equiv V_{ed}(M, 1) = V_{1+t\psi(N)}(M, 1) \equiv M \pmod{N}$$

by (2.21) and (2.11). The latter congruence follows from

$$\begin{aligned} 2V_{1+t\psi(N)}(M, 1) &= V_1(M, 1)V_{t\psi(N)}(M, 1) + DU_1(M, 1)U_{t\psi(N)}(M, 1) \\ &\equiv 2M \pmod{N}. \end{aligned}$$

The values of C and $V_d(C, 1)$ can be computed quickly by using the techniques mentioned in Sect. 3.3.

We have mentioned that if an adversary can factor N, then the RSA scheme (and LUC) can be broken. This leaves the question of whether breaking RSA is equivalent in difficulty to factoring N. Boneh and Venkatesan [9] have provided evidence which suggests that this is not the case, and Boneh and Durfee [11] have shown that if $d < N^{0.292}$, then N can be effectively factored. However, Aggarwal and Maurer [1] have proved that breaking RSA is equivalent in difficulty to factoring the modulus under a generic model of computation, but this is a very restrictive model, as it does not exploit the bit representation of elements except for testing equality. There is, nevertheless, a scheme somewhat like LUC for which it can be proved that breaking it is equivalent in difficulty to factoring N. This system, which is described in Sect. 14.2 of [32], makes use of the solutions of a certain Pell equation, which we have seen are essentially given by the Lucas functions. Further information on this system can be found in Müller [55].

References

1. D. Aggarwal and U. Maurer, *Breaking RSA generically is equivalent to factoring*, IEEE Transactions on Information Theory **62** (2016), 6251–6259.

2. M. Agrawal, N. Kayal and N. Saxena, *Primes is in P*, Annals of Math. **160**(2) (2004), 781–793.
3. E. Bach and J. O. Shallit, *Factoring with cyclotomic polynomials*, Math. Comp. **52** (1989), 201–219.
4. E. J. Barbeau, *Pell's Equation*, Springer-Verlag, NY, 2003.
5. P. Berrizbeitia and T. G. Berry, *Cubic reciprocity and generalized Lucas-Lehmer tests for primality of* $A \cdot 3^n \pm 1$, Proc. Amer. Math. Soc. **127** (1999), no. 7, 1923–1925.
6. P. Berrizbeitia, T. G. Berry and J. Tena-Ayuso, *A generalization of Proth's Theorem*, Acta Arithmetica **110.2** (2003), 107–115.
7. P. Berrizbeitia and T. G. Berry, *Biquadratic reciprocity and a Lucasian primality test*, Math. Comp. **73** (2004), 1559–1564.
8. D. Bleichenbacher, W. Bosma and A. K. Lenstra, *Some remarks on Lucas-based cryptosystems*, Advances in Cryptology-CRYPTO 95, LNCS 963, Springer-Verlag, Berlin, 1995, 386–396.
9. D. Boneh and R. Venkatesan, *Breaking RSA may not be equivalent to factoring*, Advances in Cryptology-EUROCRYPT' 98, LNCS 1403, Springer-Verlag, Berlin, 1998, 59–71.
10. Dan Boneh, *Twenty years of attacks on the RSA cryptosystem*, Notices of the AMS **46** (1999), 203–213.
11. D. Boneh and G. Durfee, *Cryptanalysis of RSA with private key d less than* $N^{0.292}$, IEEE Transactions on Information Theory **46** (2000), 1339–1349.
12. W. Bosma, *Explicit primality criteria for* $h \cdot 2^k \pm 1$, Math. Comp. **61** (1993), 97–109.
13. J. Brillhart, *Note on representing a prime as sum of two squares*, Math. Comp. **26** (1972), 1011–1013.
14. J. Brillhart, D. H. Lehmer and J. L. Selfridge, *New primality criteria and factorizations of* $2^m \pm 1$, Math. Comp. **29** (1975), 620–647.
15. J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman and S.S. Wagstaff, Jr., *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 12$ *Up to High Powers*, Contemporary Mathematics, Vol. 22, American Mathematical Society, Providence, RI, 2nd edition, 1988.
16. Johannes Buchmann, *Introduction to Cryptography*, Undergraduate Texts in Mathematics, Springer-Verlag, Berlin, 2000.
17. Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers*, Ann. of Math. (2) **163** (2006), no. 3, 969–1018.
18. C. Cailler, *Sur les congruences du troisième degré*, Enseign. Math. **10** (1908), 474–487.
19. R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math. (2) **15** (1913–1914), no. 1-4, 30–48, 49–70.
20. David A. Cox, *Primes of the Form* $x^2 + ny^2$. *Fermat, Class Field Theory and Complex Multiplication*, 2nd Edition, John Wiley & Sons, Inc., New York, 2013.

21. Richard Crandall and Carl Pomerance, *Prime Numbers: A Computational Perspective*, Springer-Verlag, New York, 2001.
22. Y. Deng and D. Huang, *Explicit primality criteria for* $h2^n \pm 1$, J. Théor. Nombres Bordeaux **28** (2016), no. 1, 55–74.
23. L. E. Dickson, *History of the Theory of Numbers*, Dover Publications, New York, 2005.
24. M. Dietzfelbinger, *Primality Testing in Polynomial Time*, Springer-Verlag, Berlin, 2004.
25. J. Franke, T. Kleinjung, F. Morain and T. Wirth, *Proving the primality of very large numbers with fast ECPP*, Algorithmic Number Theory, LNCS 3076, Springer-Verlag, Berlin, 2004, 194–207.
26. GIMPS available at https://www.mersenne.org
27. A. Granville, *It is easy to determine whether a given integer is prime*, Bull. Amer. Math. Soc. **42** (2004), no. 1, 3–38.
28. J. Grosslight, *Small skills, big networks: Marin Mersenne as mathematical intelligencer*, History of Science **51-3** (2013), 337–374.
29. R. K. Guy, *How to factor a number*, Congressus Numerantium **16** (1976), 49–89.
30. B. Ibrahimpašić, *A cryptanalytic attack on the LUC cryptosystem using continued fractions*, Mathematical Communications **14** (2009), 103–118.
31. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, NY, 1982.
32. M. J. Jacobson, Jr, and H. C. Williams, *Solving the Pell Equation*, CMS Books in Mathematics, Springer Science + Business Media, New York, 2009.
33. Philip Kaye, Raymond Laflamme and Michele Mosca, *An Introduction to Quantum Computing*, Oxford University Press, 2007.
34. D. H. Lehmer, *Tests for primality by the converse of Fermat's theorem*, Bulletin of the Amer. Math. Soc. **33** (1927), 327–340.
35. D. H. Lehmer, *On the multiple solutions of the Pell equation*, Annals of Math. **30** (1928), 66–72.
36. D. H. Lehmer, *An extended theory of Lucas' functions*, Annals of Math. **31** (1930), 419–448.
37. D. H. Lehmer, *On the Diophantine equation* $x^3 + y^3 + z^3 = 1$, J. London Math. Soc. **31** (1956), 275–280.
38. A. K. Lenstra, *Integer factoring, Designs, Codes and Cryptography* **19** (2000), 101–128.
39. H. W. Lenstra, Jr., *Solving the Pell equation*, Notices of the AMS **49** (2002), no. 2, 182–192.
40. Rudolph Lidl and Harald Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983.
41. É. Lucas, *Nouveaux théorèmes d'Arithmétique supérieure*, Comptes Rendus Acad. des Sciences, Paris, **83** (1876), 1286–1288.
42. É. Lucas, *Recherches sur plusieurs ouvrages de Leonardo de Pise et sur diverses questions d'arithmétique supérieure*, Bolletino di Bibliografia e

di Storia della Scienze Matematiche e Fisiche, **10** (1877), 129–193, 239–293.
43. É. Lucas, *Considérations nouvelles sur la théorie des nombres et sur la division géométrique de la circonférence en parties égales*, Assoc. Française pour l'Avancement des Sciences. Comptes Rendus, **6** (1877), 159–167.
44. É. Lucas, *Théorie des fonctions simplement périodiques*, Amer. J. Math. **1** (1878), 184–240, 289–321.
45. É. Lucas, *Sur la série récurrente de Fermat*, Bolletino di Bibliografia e di Storia della Scienze Matematiche e Fisiche, **11** (1878), 783–798.
46. É. Lucas, *Sur le neuvième nombre parfait*, Mathesis **7** (1887), 45–46.
47. É. Lucas, *Théorie des Nombres*, Éditions Jacques Gabay, 1991. (Authorized re-edition of the original 1891 Gauthier-Villars edition.)
48. U. M. Maurer, *Fast generation of prime numbers and secure public-key cryptographic parameters*, J. Cryptology **8** (1995), 123–155.
49. Alfred J. Menezes, Paul van Oorschot and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, 1997.
50. P. L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Math. Comp. **48** (1987), 243–264.
51. F. Morain, *Implementing the asymptotically fast version of the elliptic curve primality proving algorithm*, Math. Comp. **76** (2007), 493–505.
52. L. J. Mordell, *Diophantine Equations*, Academic Press, London, 1969.
53. S. Müller, *On the computation of square roots in finite fields*, Designs, Codes and Cryptography **31** (2004), 301–312.
54. S. Müller, *On the computation of cube roots modulo p*, High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams, Fields Inst. Communications 41, American Math. Society, Providence RI, 2004, 293–304.
55. S. Müller, *Some remarks on Williams' public-key crypto functions*, Fibonacci Quart. **44** (2006), 224–234.
56. P. Ochem and M. Rao, *Odd perfect numbers are greater than* 10^{1500}, Math. Comp. **81** (2012), 1869–1877.
57. C. Pomerance, J. L. Selfridge and S. S. Wagstaff, *The pseudoprimes up to* $25 \cdot 10^9$, Math. Comp. **35** (1980), 1003–1026.
58. J. M. Pollard, *Theorems on factorization and primality testing*, Proc. Camb. Phil. Soc. **76** (1974), 521–528.
59. R. M. Robinson, *The converse of Fermat's theorem*, Amer. Math. Monthly **64** (1957), 703–710.
60. E. L. Roettger, H. C. Williams and R. K. Guy, *Some primality tests that eluded Lucas*, Designs, Codes and Cryptography **77** (2015), 515–539.
61. E. L. Roettger and H. C. Williams, *Lucas-Lehmer primality tests for certain prime curios*, Integers **21** (2021), Article A109.
62. E. L. Roettger and H. C. Williams, *Some primality conditions for* $N = 2p^n - 1$, Integers **22** (2022), Article A76.

63. W. M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Lecture Notes in Mathematics 1467, Springer-Verlag, Berlin, 1991.
64. J. Shawe-Taylor, *Generating strong primes*, Electronics Letters 22 #16 (1986), 875–877.
65. T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Tracts in Mathematics 87, Cambridge University Press, 1986.
66. N. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Mathematical Society Student Texts 41, Cambridge University Press, 1998.
67. P. Smith, *LUC public-key encryption: a secure alternative to RSA*, Dr. Dobb's Journal, 1993, 44–48.
68. A. Stein and H. C. Williams, *Explicit primality criteria for* $(p-1)p^n-1$, Math. Comp. **69** (2000), 1721–1734.
69. J. Steuding, *Diophantine Analysis*, Chapman and Hall/CRC, Boca Raton, FL, 2005.
70. Douglas R. Stinson, *Cryptography: Theory and Practice*, Third Edition, CRC Press, Taylor and Francis Group, Boca Raton, FL, 2006.
71. J. J. Sylvester, *On certain ternary cubic-form equations*, Amer. J. Math. **2** (1879), 357–393.
72. S. S. Wagstaff, Jr., *The Joy of Factoring*, Volume 68 Student Mathematical Library, American Mathematical Society, Providence, RI, 2013.
73. H. C. Williams, *Note on a Diophantine equation*, Elemente der Mathematik , **25/6** (1970), 123–125.
74. H. C. Williams, *The primality of* $N = 2A3^n - 1$, Can. Math. Bull. **15** (1972), 585–589.
75. H. C. Williams, *A* $p+1$ *method of factoring*, Math. Comp. **39** (1982), 225–234.
76. H. C. Williams, *Effective primality tests of some integers of the forms* $A5^n - 1$ *and* $A7^n - 1$, Math. Comp. **48** (1987), 385–403.
77. H. C. Williams, *Édouard Lucas and Primality Testing*, Canadian Math. Soc. Series of Monographs and Advanced Texts, John Wiley and Sons, NY, 1998.
78. H. C. Williams and B. Schmid, *Some remarks concerning the M.I.T. public-key cryptosystem*, BIT **19** (1979), 525–538.
79. H. C. Williams and J. O. Shallit, *Factoring integers before computers*, Mathematics of Computation: A Half-Century of Computational Mathematics, Proc. Symposia in Applied Mathematics Vol. 48, AMS, Providence RI, 1993, 481–531.

Chapter 4
Some Further Properties of the Lucas Sequences

I have to change to stay the same. (Willem de Kooning)

Knowledge comes from experience, all the rest is information. (Albert Einstein)

Abstract This chapter is a compilation of some miscellaneous results involving the Lucas sequences. We begin with a discussion of the relationship of the Lucas sequences to the sine and cosine functions and then describe the periodicity properties of U and V modulo an integer m. This is followed by a section devoted to the relationship of the Lucas sequences to the Chebyshev and the Dickson polynomials. We then review some additional arithmetic properties of the Lucas sequences that are not covered in Chap. 2 and establish what Lucas called his fundamental theorem. Subsequently, we provide some insights on the factorization of the terms of U. Next, we describe Lehmer's extension of Lucas' sequences and examine some of their properties. The following section makes use of our earlier factorization results to prove an old theorem of Carmichael on primitive divisors of (U_n) and of the Lehmer sequences. We conclude with a brief treatment of the topic of when the Lucas sequence U can contain a complete set of residues modulo an integer m.

4.1 Connection with the Circular Functions

Lucas was particularly struck by the similarity of his functions to the sine and cosine functions; in fact, in Sect. II of [16], he proved that if i is used to denote a root of $x^2 + 1$, then

$$U_n = (2Q^{n/2}/\sqrt{-D}) \sin[(ni/2) \log(\alpha/\beta)]$$

© Springer Nature Switzerland AG 2023

C. J.-C. Ballot, H. C. Williams, *The Lucas Sequences*, CMS/CAIMS Books in Mathematics 8, https://doi.org/10.1007/978-3-031-37238-4_4

and

$$V_n = 2Q^{n/2}\cos[(ni/2)\log(\alpha/\beta)].$$

He did this by putting $z = n\log(\alpha/\beta)/2$ in the well-known analytic formulas

$$\sin(iz) = -(e^z - e^{-z})/2i \quad \text{and} \quad \cos(iz) = (e^z + e^{-z})/2.$$

As both sine and cosine are singly periodic functions with period 2π, Lucas (Sect. XXVI of [16]) seemed to regard U_n and V_n as simply periodic *numerical* functions, where for any particular modulus m, the (numerical) period in this case is the least positive integer $\tau = \tau(m)$ such that both

$$U_{n+\tau} \equiv U_n \pmod{m} \quad \text{and} \quad V_{n+\tau} \equiv V_n \pmod{m}$$

hold. This explains the title of [16]. He considered the above formulas as the analogues of those conveying the periodicity of the circular functions:

$$\sin(x + 2\pi) = \sin x \quad \text{and} \quad \cos(x + 2\pi) = \cos x.$$

Although Lucas was aware of the numerical periodicity of his functions modulo m, he really only proved his above numerical periodicity results when m is a prime. We will now show by a very simple process that they hold for any m such that $\gcd(m, Q) = 1$. Let (X_n) be any sequence satisfying the recursion relation (2.1), i.e.,

$$X_{n+2} = PX_{n+1} - QX_n \quad \text{for } n \geq 0.$$

If we put $T_i = (X_i, X_{i+1})$, $c_{11} = 0$, $c_{12} = -Q$, $c_{21} = 1$, and $c_{22} = P$, then $T_{i+1} = T_iC$, where $C = (c_{ij})_{2\times 2}$. Note that C is the companion matrix of $x^2 - Px + Q$ and the determinant of C, or $\det(C)$, is Q. It follows by induction that $T_n = T_0C^n$. We now assume that m is a fixed positive integer. Since there are only a finite number of residues of the integers modulo m, by the Dirichlet pigeonhole principle, there must exist some r (> 0) and s (≥ 0) such that $C^{r+s} \equiv C^s \pmod{m}$; hence, $T_{r+s} \equiv T_s \pmod{m}$. Notice that the values of r and s here are independent of the initial vector T_0. When $\det(C)$ is relatively prime to m, we see that C is invertible modulo m and therefore $C_r \equiv I \pmod{m}$, where I is the 2×2 identity matrix; in this case, we may put $s = 0$. Since for any $i \geq 0$, the vector $T_{i+1} \pmod{m}$ depends only on the vector $T_i \pmod{m}$, we must have

$$T_{n+r} \equiv T_n \pmod{m} \quad \text{for all } n \geq s,$$

and therefore,

$$X_{n+r} \equiv X_n \pmod{m} \quad \text{for all } n \geq s.$$

We call the finite sequence $(X_0, X_1, \ldots, X_{r-1})$ a *period* of (X_n) modulo m and r the length of this period.

Let $\tau \geq 1$ ($\tau = \tau(m)$) be the minimal possible value for r. Suppose that for some $\omega > 0$, we have

$$X_{n+\omega} \equiv X_n \pmod{m},$$

for all sufficiently large $n \geq 0$. Let $\omega = q\tau + \rho$, where $0 \leq \rho < \tau$. We have $X_{n+q\tau+\rho} \equiv X_n \pmod{m}$, which means by definition of τ that we must have $X_{n+\rho} \equiv X_n \pmod{m}$ for all sufficiently large n. If $\rho > 0$, this contradicts the definition of τ; hence, we must have $\tau \mid \omega$, and therefore, any period length of (X_n) modulo m must be divisible by $\tau(m)$. When $\gcd(m, Q) = 1$, we must have

$$X_{n+\tau} \equiv X_n \pmod{m},$$

for all $n \geq 0$. That is, the sequence (X_n) is purely periodic modulo m with period $(X_0, X_1, \ldots, X_{\tau-1})$. Since this is true independent of the initial vector T_0, it must hold for both $T_0 = (0, 1)$ and $T_0 = (2, P)$, which shows that Lucas' periodicity conditions hold for any m such that $\gcd(m, Q) = 1$. Also, if $X = U$, we see on putting $n = 0$ above that the rank of appearance ρ of m must, by Theorem 8, be a divisor of τ.

4.2 The Chebyshev and Dickson Polynomials

The Chebyshev polynomials crop up in just about all areas of numerical analysis. In particular, they are very important in such subjects as orthogonal polynomials, polynomial approximation, numerical integration, and spectral methods. A broad, up-to-date treatment of them can be found in Mason and Handscomb [19]. Our principal concern in this section will be the connection between these objects and the Lucas functions.

To begin, we recall the addition formulas for sine and cosine mentioned in Sect. 2.2. If we put $x = n\theta$ and $y = \theta$ and then $y = -\theta$, we get

$$\sin(n+1)\theta = \sin n\theta \cos\theta + \cos n\theta \sin\theta,\ \cos(n+1)\theta = \cos n\theta \cos\theta - \sin n\theta \sin\theta$$

and

$$\sin(n-1)\theta = \sin n\theta \cos\theta - \cos n\theta \sin\theta,\ \cos(n-1)\theta = \cos n\theta \cos\theta + \sin n\theta \sin\theta.$$

On adding, we get

$$\begin{aligned} \sin(n+1)\theta &= 2\sin n\theta \cos\theta - \sin(n-1)\theta, \\ \cos(n+1)\theta &= 2\cos n\theta \cos\theta - \cos(n-1)\theta. \end{aligned} \tag{4.1}$$

We observe that since $\sin 2\theta = 2\sin\theta\cos\theta$, $\cos 2\theta = 2\cos^2\theta - 1$, we can easily prove by induction that for any fixed nonnegative n, there exist integer constants a_i, b_i $(i = 0, 1, 2, \ldots, n)$ such that

$$\sin(n+1)\theta = \sin\theta \sum_{i=0}^{n} a_i(\cos\theta)^i, \quad \cos n\theta = \sum_{i=0}^{n} b_i(\cos\theta)^i.$$

It follows that for each nonnegative integer n, there exist two polynomials of degree n with integer coefficients, $T_n(x)$ and $U_n(x)$, such that

$$\sin(n+1)\theta = \sin\theta \cdot U_n(\cos\theta), \quad \cos n\theta = T_n(\cos\theta).$$

We call $T_n(x)$ the Chebyshev polynomial of the first kind and $U_n(x)$ the Chebyshev polynomial of the second kind. Note that $T_0(x) = U_0(x) = 1$, $T_1(x) = x$, and $U_1(x) = 2x$. Also, from (4.1), it is easy to deduce that

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x) \quad \text{and} \quad U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x), \tag{4.2}$$

$(n = 1, 2, 3, \dots)$. From the initial conditions on T_n and U_n and (4.2), we find that

$$2T_n(x) = V_n(2x, 1), \quad U_n(x) = U_{n+1}(2x, 1). \tag{4.3}$$

These are the relationships which connect the Chebyshev polynomials to the Lucas functions with $P = 2x$ and $Q = 1$. Thus, any identity involving the Lucas functions can be used to find a corresponding identity which involves the Chebyshev polynomials. For example, from (2.8), we get

$$T_n(x)^2 - (x^2 - 1)U_{n-1}(x)^2 = 1;$$

hence, by the results in Sect. 3.6, we see that the successive solutions of the Pell equation with $d = x^2 - 1$, starting with $(x, 1)$, are provided by $(T_n(x), U_{n-1}(x))$ with $n \geq 1$. Also, since $V_{mn}(P, Q) = V_n(V_m, Q^m)$ by (2.21), we see that $T_{mn}(x) = T_n(T_m(x))$; this result is an important ingredient in a public-key encryption scheme promoted by Kocarev et al. [11]. By the first identity in (2.26), we have $V_n = U_{n+1} - QU_{n-1}$; hence, by (4.3), we get

$$2T_n(x) = U_n(x) - U_{n-2}(x). \tag{4.4}$$

Notice that the derivatives $T_1'(x) = 1 = U_0(x)$ and $T_2'(x) = 4x = 2U_1(x)$. Suppose that $T_n'(x) = nU_{n-1}(x)$ and $T_{n-1}'(x) = (n-1)U_{n-2}(x)$; this is certainly true for $n = 2$. If we take the derivative with respect to x of the first formula of (4.2), we get

$$\begin{aligned} T_{n+1}'(x) &= 2T_n(x) + 2xT_n'(x) - T_{n-1}'(x) \\ &= U_n(x) - U_{n-2}(x) + 2xnU_{n-1}(x) - (n-1)U_{n-2}(x) \\ &= U_n(x) + n(2xU_{n-1}(x) - U_{n-2}(x)), \end{aligned}$$

by our supposition and (4.4). By the second formula of (4.2), we find that $T_{n+1}'(x) = (n+1)U_n(x)$; thus, we have proved by induction that

$$T_n'(x) = nU_{n-1}(x) \quad (n = 1, 2, 3, \dots). \tag{4.5}$$

Some years ago, some use was made of the modified Chebyshev polynomials, $C_n(x)$ and $S_n(x)$; these were defined as

$$C_n(x) = 2T_n(x/2), \quad S_n(x) = U_n(x/2). \tag{4.6}$$

We note from (4.3) that

$$C_n(x) = V_n(x, 1), \quad S_n(x) = U_{n+1}(x, 1); \tag{4.7}$$

hence, $C_0(x) = 2$, $S_0(x) = 1$, $C_1(x) = x = S_1(x)$, and

$$C_{n+1}(x) = xC_n(x) - C_{n-1}(x), \quad S_{n+1}(x) = xS_n(x) - S_{n-1}(x), \tag{4.8}$$

for $n \geq 1$. Although these degree n polynomials are monic for $n > 0$ and have some nice algebraic properties, they never seemed to catch on with the numerical analysis community (see [19, p. 11]). Also, the S and C notation seems to have been largely abandoned, and it is now customary to use Ω instead of C and V instead of S. Several properties and applications of $\Omega_n(x)$ and $V_n(x)$, together with references, can be found in Wituła and Słota [40]. We will prove some results concerning them below, but because of possible confusion between $V_n(x)$ and $V_n(x, 1)$, we will revert back to the earlier notation. We first note that

$$\begin{aligned} &\Omega_n(x + x^{-1}) = C_n(x + x^{-1}) = V_n(x + x^{-1}, 1) = x^n + x^{-n}; \\ &S_n(x + x^{-1}) = U_{n+1}(x + x^{-1}, 1) = (x^{n+1} - x^{-n-1})/(x - x^{-1}). \end{aligned} \tag{4.9}$$

By the Girard-Waring formula (2.37), we have for $n > 0$

$$C_n(x) = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \frac{n}{n-k} \binom{n-k}{k} x^{n-2k}. \tag{4.10}$$

By the first formula of (4.6) and (4.5), we can easily derive $C_n'(x) = nS_{n-1}(x)$; hence, by differentiating (4.10), we can readily deduce that

$$S_n(x) = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \binom{n-k}{k} x^{n-2k}. \tag{4.11}$$

Note that by putting $x = (\alpha/\beta)^{m/2} = \alpha^m/Q^{m/2}$, then (4.9) together with (4.10) and (4.11) can be used to derive multiplication formulas for the Lucas functions. Additional formulas can be found by putting $x = \alpha^m/(-Q)^{m/2}$; for example, when n is positive and $n = 2r$, we can use the second formula of (4.9), formula (4.11), and sum over $j = r - k - 1$ to obtain

$$U_{2rm} = V_m \sum_{j=0}^{r-1} \binom{r+j}{r-j-1} D^j Q^{m(r-j-1)} U_m^{2j+1}. \tag{4.12}$$

Other, similar formulas can also be derived in this way. See Sect. 4.2 of [39]. We also see from (2.21) and (4.7) that

$$C_{nm}(x) = C_m(C_n(x)). \tag{4.13}$$

The degree n polynomial $G_n(x)$ introduced in Sect. 3.3 satisfies the same recurrence as $S_n(x)$. Thus, since $1 = G_0(x) = S_0(x) + S_{-1}(x)$ and $x + 1 = G_1(x) = S_1(x) + S_0(x)$, it is easy to see that

$$G_n(x) = S_n(x) + S_{n-1}(x), \tag{4.14}$$

for $n \geq -1$. By using (4.14) and (4.11), we find that

$$G_n(x) = \sum_{i=0}^{n} (-1)^{\lfloor i/2 \rfloor} \binom{n - \lfloor (i+1)/2 \rfloor}{\lfloor i/2 \rfloor} x^{n-i}.$$

Also, by (4.14) and the second formula of (3.8), we get

$$G_n(x) + G_{n-1}(x) = (x+2)S_{n-1}(x), \tag{4.15}$$

and by (4.4) and (4.6), we have

$$G_n(x) - G_{n-1}(x) = C_n(x); \tag{4.16}$$

from this result, it follows easily that we can write

$$G_n(x) = 1 + \sum_{j=1}^{n} C_j(x). \tag{4.17}$$

Since, by (2.16), we have

$$U_{n+m}(x,1) = V_n(x,1)U_m(x,1) - U_{m-n}(x,1),$$

we can use (4.7) to derive

$$\begin{aligned} S_{n+m-1}(x) &= C_n(x)S_{m-1}(x) - S_{m-n-1}(x), \\ S_{n+m}(x) &= C_n(x)S_m(x) - S_{m-n}(x). \end{aligned}$$

On adding these and using (4.14) and (4.16), we get the addition formula for $G_n(x)$:

$$G_{m+n}(x) = G_n(x)G_m(x) - G_{n-1}(x)G_m(x) - G_{m-n}(x). \tag{4.18}$$

Particular instances of this formula are

$$\begin{aligned} G_{2m+2}(x) &= G_{m+1}(x)^2 - G_{m+1}(x)G_m(x) - 1, \\ G_{2m+1}(x) &= G_{m+1}(x)G_m(x) - G_m(x)^2 + 1. \end{aligned} \tag{4.19}$$

Also, since $G_{m-1}(x) = xG_m(x) - G_{m+1}(x)$, we have

$$G_{2m}(x) = G_{m+1}(x)G_m(x) - (x-1)G_m(x)^2 - 1. \tag{4.20}$$

Formulas (4.19) and (4.20) can be used in the manner discussed in Sect. 3.3 to produce a fast method to compute $G_n(x)$ for large values of n; this, in view of (3.7) and (3.8), provides a rapid technique for computing the Lucas quotients V_{rn}/V_n and $U_{rn}/U_n \pmod N$ when r is large and odd.

We next turn our attention to the Dickson polynomials. These polynomials are generally used in the study of finite fields, where they provide many examples of permutation polynomials; such polynomials induce permutations on the finite field $\mathbb{F}_q$ of q elements. Much more concerning this topic can be found in Chap. 7 of Lidl and Niederreiter [14] and in Mullen and Panario [21]. We will confine our discussion here to the relationship between the Dickson polynomials and the Lucas functions.

For a positive integer n and a fixed $a \in \mathbb{F}_q$, we define the nth Dickson polynomial of the first kind $D_n(x,a)$ over $\mathbb{F}_q$ by

$$D_n(x,a) = \sum_{k=0}^{\lfloor n/2 \rfloor} (-a)^k \frac{n}{n-k} \binom{n-k}{k} x^{n-2k}.$$

We define the nth Dickson polynomial of the second kind $E_n(x,a)$ over $\mathbb{F}_q$ by

$$E_n(x,a) = \sum_{k=0}^{\lfloor n/2 \rfloor} (-a)^k \binom{n-k}{k} x^{n-2k}.$$

Notice that these polynomials are monic and of degree n over $\mathbb{F}_q$. From the definitions, we see immediately from (2.34) and (2.30) that

$$D_n(x,a) = V_n(x,a), \quad E_n(x,a) = U_{n+1}(x,a). \tag{4.21}$$

Many characteristics of the Dickson polynomials can be found in Lidl et al. [15], but in view of (4.21), several of these can be derived from the properties of the Lucas functions. For example, we have $D_0(x,a) = 2$, $E_0(x,a) = 1$, and $D_1(x,a) = x = E_1(x,a)$, and from (4.21) and (2.1), we get the recursive formulas:

$$D_{n+1}(x,a) = xD_n(x,a) - aD_{n-1}(x,a),\ E_{n+1}(x,a) = xE_n(x,a) - aE_{n-1}(x,a).$$

From (4.3), it is easy to see that the Dickson polynomials are related to the Chebyshev polynomials by

$$D_n(2x,1) = 2T_n(x), \quad E_n(2x,1) = U_n(x).$$

From the remarks in Sect. 3.7 and earlier in this section, the above relationships suggest that the Dickson polynomials could be applied to public-key cryptography; indeed, this was done as early as 1981 by Müller and Nöbauer [22]. For a more modern treatment of several of the two-key cryptosystems mentioned in this section and in Sect. 3.7, the reader is referred to Brandner [3].

4.3 Some Additional Arithmetic Properties of the Lucas Sequences

In Chap. 2, we derived a number of arithmetic properties of the Lucas sequences, but there are many more such results. In this section, we will detail some of these. We set out by observing that if $n, m \geq 1$ and m is odd, then by Theorem 4, we have $V_n \mid V_{mn}$. Furthermore, by (2.36), we find that

$$V_{mn}/V_n \equiv (-1)^{(m-1)/2} Q^{n(m-1)/2} \pmod{V_n};$$

hence,

$$\gcd(V_{mn}/V_n, V_n) \mid mQ^{n(m-1)/2}.$$

There is a similar result for U.

Theorem 60 *If $n, m \geq 1$, we have*

$$\gcd(U_{mn}/U_n, U_n) \mid mQ^{n\lfloor m/2 \rfloor}.$$

Proof If m is odd, we have from (2.38)

$$U_{mn}/U_n \equiv mQ^{n(m-1)/2} \pmod{U_n},$$

and the result follows easily in this case. We now turn to the case of m even. If $m = 2r$, we get

$$U_{mn}/U_n \equiv rV_nQ^{n(r-1)} \pmod{U_n}$$

by (4.12). It follows that $\gcd(U_{mn}/U_n, U_n) \mid \gcd(rV_nQ^{n(r-1)}, U_n)$. Since $\gcd(rV_nQ^{n(r-1)}, U_n)$ must divide $rQ^{n(r-1)} \gcd(V_n, U_n)$, we see that $\gcd(U_{mn}/U_n, U_n)$ must divide $2rQ^{rn}$ by Lemma 4. The result now follows for even m. □

If U is regular ($\gcd(P, Q) = 1$), then, by Lemma 3, we have

$$\gcd(V_{mn}/V_n, V_n) = 1 \quad \text{and} \quad \gcd(U_{mn}/U_n, U_n) \mid m.$$

These results seem not to have been known to Lucas; the latter was first proved for m a prime by Carmichael in [7, p. 51], using a different approach.

We next look at Lucas' [16, Sect. XXVI] generalization of Euler's φ function (see also the discussion in Sect. 2.6). For any U and any prime p such that $p \nmid Q$, we define $\varphi_U(p^k)$ by $\varphi_U(p^k) = p^{k-1}(p - \epsilon_p)$, where ϵ_p is the value of the Legendre symbol $(D \mid p)$. By our results in Sects. 2.4 and 2.5, we have $p^k \mid U_f$, where $f = \varphi_U(p^k)$. If $n \geq 1$ and $\gcd(n, Q) = 1$, we define the multiplicative function $\varphi_U(n)$ as

$$\varphi_U(n) = \prod \varphi_U(p^k),$$

where the product is taken over all p^k such that $p^k \,||\, n$. Notice that if D is a perfect square and $\gcd(n, QD) = 1$, we have $\varphi_U(n) = \varphi(n)$.

For any positive integer n coprime to Q, we have $n \mid U_{\varphi_U(n)}$, and therefore, by Theorem 8, we get $\rho(n) \mid \varphi_U(n)$. We observe further that if we define $\Lambda(n)$ to be the least common multiple of $\varphi_U(p^k)$ for all p^k such that $p^k \,||\, n$, then we must have $n \mid U_{\Lambda(n)}$ and $\rho(n) \mid \Lambda(n)$. If n is odd and $\gcd(n, QD) = 1$, then $2 \mid \varphi_U(p^k)$; thus, in this case, $\Lambda(n) \mid \varphi_U(n)/2^{t-1}$, where t is the number of distinct prime divisors of n.

We next establish the following technical lemma.

Lemma 23 *If n is odd, $\gcd(n, QD) = 1$, and n has $t \geq 2$ distinct prime factors, then $\varphi_U(n)/2^{t-1} \leq n - 1$.*

Proof Since $t \geq 2$, we have

$$\frac{\varphi_U(n)}{n} = \prod \left(1 - \frac{\epsilon_p}{p}\right) \leq \left(1 + \frac{1}{3}\right)\left(1 + \frac{1}{5}\right)2^{t-2} = \frac{4}{5} \cdot 2^{t-1};$$

it follows that $\varphi_U(n)/2^{t-1} \leq 4n/5 < n - 1$, because n has at least 2 distinct odd prime factors and must, as a consequence, be at least as large as 15. □

We are now able to prove the theorem whose proof gave Lucas so much trouble.

Theorem 61 *Suppose U is regular. If n is odd, $\gcd(n, Q) = 1$, and $\rho(n) = n - \gamma$, where $|\gamma| = 1$, then n is a prime.*

Proof Suppose n is composite and that $\gcd(n, D) > 1$. We must have some odd prime q such that $q \mid n$ and $q \mid D$. Since $q \mid U_{n-\gamma}$, we must have $\rho(q) \mid n - \gamma$ by Theorem 8. Also, by Theorem 9, we have $\rho(q) = q$, which is impossible because $\gcd(n, n - \gamma) = 1$. It follows that we must have $\gcd(n, D) = 1$. Since $\rho(n) \mid \Lambda(n)$ and $\Lambda(n) \leq \varphi_U(n)/2^{t-1} < n - 1$ by the lemma, we get a contradiction. □

The above result can be used to prove Lucas' fundamental theorem mentioned in Sect. 3.2.

Theorem 62 *If n is odd, U is regular, and $n \mid U_{n-\gamma}$, where $|\gamma| = 1$, but $n \nmid U_d$ for all aliquot divisors d of $n - \gamma$, then n is a prime.*

Proof Since U is regular, by Lemma 2, we have $\gcd(U_n, Q) = 1$. Also, since $n \nmid U_d$ for all aliquot divisors d of $n - \gamma$, we must have $\rho(n) = n - \gamma$. The theorem now follows from Theorem 61. □

We next concern ourselves with how the numbers in the Lucas sequence U can be factored. As pointed out in Sect. 3.5, the general problem of integer factorization is considered to be very difficult, but, as noticed by Carmichael [7], the Lucas functions U_n possess some distinctive properties, which allow them to be represented as a product of some special integers. In order to find this representation, we first consider the cyclotomic polynomials $\Phi_n(x)$, mentioned at the end of Sect. 3.5, in greater detail. We define $\Phi_n(x)$ to be the unique polynomial with integer coefficients which divides $x^n - 1$, but does not divide $x^k - 1$ for any positive integer $k < n$. The roots of $\Phi_n(x)$ must therefore be the $\varphi(n)$ primitive nth roots of unity, and we can write

$$\Phi_n(x) = \prod (x - \zeta^k) \tag{4.22}$$

where ζ is some primitive nth root of unity ($e^{2\pi i/n}$ is such a root) and the product is taken over all integral $k \geq 1$ such that $\gcd(k, n) = 1$ and $k < n$. It follows that $\Phi_n(x)$ is monic and its degree is $\varphi(n)$. We also see that since

$$\sum_{d|n} \varphi(d) = n, \tag{4.23}$$

we get

$$x^n - 1 = \prod_{d|n} \Phi_d(x), \tag{4.24}$$

where the product is taken over all the positive divisors d of n. Furthermore, Gauss showed that the cyclotomic polynomials are irreducible over the rationals (see, e.g., Weintraub [37]).

Let μ denote the Möbius function defined by $\mu(1) = 1$ and for $n \geq 2$

$\mu(n) = 1$, if n is square-free with an even number of prime factors.
$\mu(n) = -1$, if n is square-free with an odd number of prime factors.
$\mu(n) = 0$, if n has a squared prime factor.

By Möbius inversion applied to functions written as products, we find from (4.24) that

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)} = \prod_{d|n} (1 - x^{n/d})^{\mu(d)}, \tag{4.25}$$

where, as before, the product is taken over all the positive divisors d of n. The last equality in (4.25) follows from $\sum_{d|n} \mu(d) = 0$ when $n > 1$. For more information concerning $\Phi_n(x)$ and examples, see Appendix 6 of Riesel [25];

results involving the Möbius function can be found, for example, in Sect. 3.5 of Shapiro [30].

We now define the sequence of numbers $(Q_n)_{n\geq 1}$, called the cyclotomic numbers associated with $U_n(P,Q)$, by putting $Q_1 = 1$ and for $n \geq 2$,

$$Q_n = Q_n(\alpha,\beta) = \prod(\alpha - \zeta^k\beta), \tag{4.26}$$

where ζ is some primitive nth root of unity and the product is taken over all integral $k \geq 1$ such that $\gcd(k,n) = 1$ and $k < n$. For example, $Q_2 = \alpha+\beta = P$ and $Q_3 = \alpha^2 + \alpha\beta + \beta^2 = P^2 - Q$. By (4.22), we have for $n \geq 2$

$$Q_n = Q_n(\alpha,\beta) = \beta^{\varphi(n)}\Phi_n(\alpha/\beta). \tag{4.27}$$

Thus, $Q_n(\alpha,\beta)$ can be regarded as a polynomial in α and β with integral coefficients. If we put $x = \alpha/\beta$ in (4.22), we see by (4.27) that

$$(\alpha/\beta)^n - 1 = (\alpha/\beta - 1)Q_1 \prod \beta^{-\varphi(d)}Q_d,$$

where the product is taken over all divisors $d \geq 2$ of n. By (4.23), we find that

$$U_n = \prod_{d|n} Q_d. \tag{4.28}$$

Notice that if $n > 2$ and $1 \leq k < n$, then $1 \leq n-k < n$ and $\gcd(k,n) = \gcd(n-k,n)$. It follows that $n \mid \sum k$, where the sum is taken over all integral $k \geq 1$ such that $\gcd(k,n) = 1$ and $k < n$. Thus, if $n > 2$, we have $2 \mid \varphi(n)$, and we can write (4.26) as

$$\begin{aligned} Q_n(\alpha,\beta) &= \prod(\alpha - \zeta^k\beta) = \prod(\zeta^k\beta - \alpha) = \prod(\beta - \zeta^{-k}\alpha) \\ &= \prod(\beta - \zeta^{n-k}\alpha) = \prod(\beta - \zeta^k\alpha) = Q_n(\beta,\alpha). \end{aligned}$$

Since $Q_n(\alpha,\beta)$ is an integral polynomial in α,β and symmetric with respect to α,β, we see that for any integers P and Q, we must have Q_n an integer for $n \geq 1$. Hence, the formula (4.28) expresses U_n as a product of integers.

At this point, we should mention that Lucas [17, 18] observed that certain formulas for $\Phi_n(x)$, which he attributed to Aurifeuille and Le Lasseur, could be used to derive identities involving the Lucas sequences and for factoring some of these expressions. For example, in [18], he gave the identity

$$V_{10n}/V_{2n} = (V_{4n} + 5Q^nV_{2n} + 7Q^{2n})^2 - 10Q^n(V_{3n} + 2Q^nV_n)^2.$$

He derived this from the Aurifeuillian formula

$$\Phi_{20}(x) = \frac{x^{10}+1}{x^2+1} = (x^4 + 5x^3 + 7x^2 + 5x + 1)^2 - 10x(x^3 + 2x^2 + 2x + 1)^2,$$

by putting $x = \alpha^n/\beta^n$, where $\alpha + \beta = P$ and $\alpha\beta = Q$. Notice that this formula for V_{10n}/V_n will factor as a difference of squares when $10Q^n$ is a perfect square. This means that n should be odd and $Q = 10L^2$, where L is an integer.

Other results, apparently not known to Lucas, can be found by substituting other expressions involving α^n/β^n for x in Aurifeuillian formulas. As an example, consider

$$\Phi_5(x) = \frac{x^5 - 1}{x - 1} = (x^2 + 3x + 1)^2 - 5x(x + 1)^2,$$

a formula known to Lucas. If we put $x = (-\alpha^n/\beta^n)^{1/2}$, we get

$$\begin{aligned}\frac{V_{5n}}{V_n} &= (V_n^2 - 5Q^n)^2 + 5Q^n DU_n^2 \\ &= (DU_n^2 - Q^n)^2 + 5Q^n DU_n^2.\end{aligned}$$

If $-5Q^n D$ is a perfect integral square, we have a factorization of V_{5n}/V_n. Suppose we have integers M, L, and S such that

$$M^2 + 4L^2 = 5S^2,$$

and put $P = M$ and $Q = -L^2$. We find that $D = 5S^2$ and $-5Q^n D = -25(-L^2)^n$, a perfect square when n is odd. If we consider the special case of $M = L = S = 1$, we get the pretty identity found by Jarden [10, Sect. 8]:

$$L_{5n}/L_n = (5F_n^2 - 5F_n + 1)(5F_n^2 + 5F_n + 1),$$

for an odd n. This result was enlisted by Brillhart, Montgomery, and Silverman [4] to assist in compiling a table of integer factorizations of Lucas numbers. It has been generalized recently by Roettger and Williams [26].

For recent information concerning Aurifeuillians and additional references, the reader is advised to consult Granville and Pleasants [9] and Wagstaff [34, Sect. 4.1]. For some historical commentary, see [39, pp. 126–127, 318–319].

Let N be any odd positive integer. In Sect. 3.2, we defined N to be a base a pseudoprime if N is composite and satisfies $\gcd(a, N) = 1$ and (3.1). It is a remarkable fact that there exist composite N which satisfy (3.1) for all a such that $\gcd(a, N) = 1$; such numbers are called absolute pseudoprimes or, more frequently, *Carmichael numbers*. It has been known since 1899 (Sect. 3.3.2 of Crandall and Pomerance [8]) that a positive integer N is a Carmichael number if and only if N is composite and square-free and such that $p - 1 \mid N - 1$ for each prime p which divides N. For example, $N = 561 = 3 \cdot 11 \cdot 17$ is the smallest Carmichael number. These numbers have been tabulated by Pinch [24] up to 10^{21}.

We also mentioned in Sect. 3.2 the definition of a Lucas pseudoprime; we can extend this to a Lucas function analogue of the Carmichael numbers as follows:

For a fixed D, we say that a composite N is an *absolute Lucas D-pseudoprime* if for all P and Q such that $\gcd(P, Q) = \gcd(N, QD) = 1$ and $P^2 - 4Q = D$, we have

$$U_{N-\epsilon(N)}(P, Q) \equiv 0 \pmod{N},$$

where $\epsilon(N)$ is the value of the Jacobi symbol $(D \mid N)$. In Williams [38], it was shown that if for a fixed D, N is an absolute Lucas D-pseudoprime, it is necessary that N be square-free and $p - \epsilon_p \mid N - \epsilon(N)$ for each prime divisor p of N. Since $\rho(p) \mid p - \epsilon_p$, these conditions are also clearly sufficient for N to be an absolute Lucas D-pseudoprime. Thus, we see that an absolute Lucas 1-pseudoprime must be a Carmichael number, and therefore, the absolute Lucas D-pseudoprimes represent a special case of the Carmichael numbers. Very recently, Webster and Gurovski [36] have computed all the absolute Lucas 5-pseudoprimes up to 10^{15}. It is still unknown whether there exist any N and D such that $(D \mid N) = \epsilon(N) = -1$ and N is both a Carmichael number and an absolute Lucas D-pseudoprime. It is shown in [38] that such values of N must be the product of an odd number of distinct primes p satisfying $p - 1 \mid N - 1$ and $p + 1 \mid N + 1$. A search up to 10^{16} conducted by Pinch [23] did not produce such an N. More recent work of McIntosh and Dipra [20] extended this bound to 2×10^{19}, but still found no value for N. Many refinements of the ideas presented here, together with several references, can also be found in [20, 23] and Shallue and Webster [29].

4.4 The Lehmer Sequences

Suppose R, $Q \neq 0$ and $\gcd(R, Q) = 1$. In [12], Lehmer extended the regular Lucas sequences by replacing the integer P by $\sqrt{R}$, where R is an integer. In this case, we have $D = R - 4Q$, which means that D can be 2 or 3 (mod 4), something that is impossible for the Lucas sequences. Of course, if R is not a perfect square, then we see from (2.1) that $U_n(\sqrt{R}, Q)$ and $V_n(\sqrt{R}, Q)$ are not always going to be integers for $n \geq 1$. If we define

$$\bar{U}_n(R, Q) = U_n(\sqrt{R}, Q), \quad \bar{V}_n(R, Q) = V_n(\sqrt{R}, Q)/\sqrt{R} \qquad (2 \nmid n)$$

and

$$\bar{U}_n(R, Q) = U_n(\sqrt{R}, Q)/\sqrt{R}, \quad \bar{V}_n(R, Q) = V_n(\sqrt{R}, Q) \qquad (2 \mid n),$$

then it is easy to see from (2.18) that both $(\bar{U}_n(R, Q))$ and $(\bar{V}_n(R, Q))$ satisfy the fourth-order recurrence

$$X_{n+4} = (R - 2Q)X_{n+2} - Q^2 X_n.$$

Since $\bar{U}_0(R,Q) = 0$, $\bar{U}_1(R,Q) = \bar{U}_2(R,Q) = 1$, $\bar{U}_3(R,Q) = R - Q$, and $\bar{V}_0(R,Q) = 2$, $\bar{V}_1(R,Q) = 1$, $\bar{V}_2(R,Q) = R - 2Q$, $\bar{V}_3(R,Q) = R - 3Q$, we see by induction that $U_n(\sqrt{R},Q)$ and $V_n(\sqrt{R},Q)$ will always be integers whenever $n \geq 0$.

We call the sequences $\bar{U} = (\bar{U}_n(R,Q))$ and $\bar{V} = (\bar{V}_n(R,Q))$ the *Lehmer sequences*. Since the identity relations given in Chap. 2 hold for non-integral values of P and Q, it is possible to derive several properties of these sequences which are analogous to corresponding results concerning the Lucas sequences. For example, we easily find from (2.23) and (2.24) that

$$\begin{aligned}
\bar{U}_{2n}(R,Q) &= \bar{V}_n(R,Q) \cdot \bar{U}_n(R,Q);\\
\bar{V}_{2n}(R,Q) &= \bar{V}_n(R,Q)^2 - 2Q^n, \text{ if } 2 \mid n;\\
\bar{V}_{2n}(R,Q) &= R\,\bar{V}_n(R,Q)^2 - 2Q^n, \text{ if } 2 \nmid n;
\end{aligned}$$

From the identity (2.8), it is easy to derive

$$R\bar{V}_n^2 - D\bar{U}_n^2 = 4Q^n,$$

whenever n is odd, and

$$\bar{V}_n^2 - DR\bar{U}_n^2 = 4Q^n,$$

whenever n is even. Indeed, if s denotes an odd integer, we can produce the additional identities

$$\begin{aligned}
\bar{V}_s^2 - D\bar{U}_{s-1}\bar{U}_{s+1} &= Q^{s-1},\\
D\bar{U}_s^2 - \bar{V}_{s-1}\bar{V}_{s+1} &= -RQ^{s-1},
\end{aligned}$$

which will be useful in Sect. 8.5. These follow from the easily verified Lucas sequence identities

$$V_n^2 - DU_{n+1}U_{n-1} = P^2Q^{n-1} = V_{n-1}V_{n+1} - DU_n^2.$$

Lehmer was also able to show that $\bar{U}$ is a strong divisibility sequence and if $\omega = \omega(m)$ is the rank of appearance of the integer m in $\bar{U}$, then $\omega \mid n$ whenever $m \mid \bar{U}_n(R,Q)$. Using (2.28) and (2.29), he also showed that if p is an odd prime and $p \nmid Q$, then

$$\bar{U}_p \equiv (D \mid p) = \epsilon_p \pmod{p}, \quad \bar{V}_p \equiv (R \mid p) \pmod{p}.$$

By using (2.10), (2.12), (2.11), and (2.13), with $m = p$ and $n = 1$, and the above congruences, he deduced that

$$p \mid \bar{U}_{p-\epsilon\sigma}(R,Q) \quad \text{and} \quad \bar{V}_{p-\epsilon\sigma}(R,Q) \equiv 2\sigma Q^{(1-\epsilon\sigma)/2} \pmod{p},$$

where $\epsilon = \epsilon_p := (D \mid p)$ and $\sigma = \sigma_p := (R \mid p)$. It follows that $\omega(p) \mid p - \epsilon\sigma$. From these results, we can produce a law of appearance for $\bar{U}_n(R, Q)$ whenever $p \nmid RQ$, and if $p \mid R$, $p \nmid Q$, we get $p \mid \bar{U}_{2p}(R, Q)$. Lehmer also proved a result similar to Theorem 2.10.1.

Theorem 63 *Define $\tau = \tau_p := (Q \mid p)$. If p is an odd prime and $p \nmid DQR$, then $p \mid \bar{V}_{(p-\sigma\epsilon)/2}$ if and only if $\sigma = -\tau$.*

With these findings, he was able to prove Theorem 50 (the Lucas-Lehmer test) by putting $R = 2$ and $Q = -1$. (See Theorem 8.4.9 in [39].)

We can also derive results concerning the $\bar{V} = \bar{V}(R, Q)$ sequence which are analogous to those proved for the V sequence in Chap. 2; for example, $\gcd(\bar{V}_n, Q) = 1$, $\gcd(\bar{U}_n, \bar{V}_n) = 1$ or 2, and $\bar{V}_n \mid \bar{V}_{nm}$ whenever m is positive and odd. Indeed, by using the same kind of reasoning as that employed in Sect. 2.7, we can show further that if p is some odd prime such that $p \nmid Q$ and $\chi\ (= \chi(p))$ (if it exists) is the least positive value of n such that $p \mid \bar{V}_n$, then $\omega(p)$ must be even and $\chi = \omega/2$. Also, if $p \nmid RQ$ and $p \mid \bar{V}_m$, then $\chi \mid m$ and m/χ is odd. Thus, if $p \nmid DQR$ and $\chi(p)$ exists, then $\chi(p)$ must be a divisor of $(p - \epsilon\sigma)/2$.

For any odd prime p such that $p \nmid Q$ and any positive integer k, we define $W(p^k) = p^{k-1}(p - (RD \mid p))$. For any $n \geq 1$ and $\gcd(n, Q) = 1$, Lehmer defined his generalization $T(n)$ of Euler's totient function as

$$T(n) = 2 \prod W(p^k),$$

where the product is taken over all p^k such that $p^k \,||\, n$. By the laws of appearance and repetition for the Lehmer sequences, we have

$$\bar{U}_{T(n)} \equiv 0 \pmod{n},$$

for any positive integer n such that $\gcd(n, Q) = 1$. Lehmer also defined $S(n)$ to be the least common multiple of the factors 2 and $W(p^k)$ of $T(n)$ and noted that $n \mid \bar{U}_{S(n)}$; therefore, $\omega(n) \mid S(n)$ for any positive integer n such that $\gcd(n, Q) = 1$. Thus, by using the methods of Sect. 4.3, we can prove a result completely analogous to Theorem 61 for the Lehmer sequence $\bar{U}$.

4.5 The Primitive Divisor Theorem

Let $X = (X_n)_{n \geq 0}$ be any integer sequence. If p is a prime such that $p \mid X_n$ but $p \nmid X_m$ for any $m < n$, we say that p is a *primitive divisor* of X_n. As an example, consider the Fibonacci sequence, where we get $F_n = 55$ when $n = 10$. Since the aliquot divisors of 10 are 1, 2, and 5 and $F_1 = F_2 = 1$ and $F_5 = 5$, we see that 11 must be a primitive divisor of F_{10}. Indeed, if U is a Lucas sequence and $n > 1$, we see that p is a primitive divisor of U_n

if and only if $\rho(p) = n$. Notice that it is not always the case that any U_n with $n > 1$ will have a primitive divisor. For example, consider $F_{12} = 144$; there are only two primes 2 and 3 which divide this number and $\rho(2) = 3$ and $\rho(3) = 4$ for the Fibonacci sequence. For a given U, it is of some interest to determine those values of n such that U_n contains a primitive divisor. For a general Lucas sequence, this turns out to be a very deep and difficult problem which has only recently been solved. However, in the case of $D > 0$, the problem was solved by Carmichael [7] in 1913. Yabuta [41] has provided an elementary and relatively simple proof of Carmichael's result, which we will sketch below. We will assume in what follows that U is regular. Since we are dealing with primes that divide some term U_n with $n > 0$, we may also assume that $p \nmid Q$. We first observe that by using (2.1), it is easy to establish by induction on n that

$$U_n(-P, Q) = (-1)^{n-1} U_n(P, Q), \quad V_n(-P, Q) = (-1)^n V_n(P, Q) \tag{4.29}$$

for $n \geq 0$. Thus, whatever the sign of D, we may always assume that $P > 0$.

By (4.28), it is easy to see that p is a primitive divisor of U_n if and only if p is a primitive divisor of Q_n. We now prove some preliminary lemmas.

Lemma 24 *Let p be a prime such that p divides U_n with $n > 0$. If $p \mid Q_n$, then $n = \rho(p)p^k$, where k is a nonnegative integer and $\rho(p) > 0$ is the rank of appearance of p in U.*

Proof Since $p \mid U_n$, by Theorem 8, we have $n = r\rho(p)p^k$, where $p \nmid r$ and $k \geq 0$. Put $m = \rho(p)p^k$ and let $p^\nu \,||\, U_m$. Since $\rho(p) \mid m$, we must have $\nu \geq 1$; by Corollary 11 and results in Sect. 2.5, we see that $4p \nmid U_n/U_m$. From (4.28), we also see that $Q_n \mid U_n/U_m$ when $r > 1$, but since $p|Q_n$, this is impossible. It follows that we can only have $r = 1$ and $n = \rho(p)p^k$. □

Lemma 25 *Let $\rho(p) > 0$ be the rank of appearance of p in U. For any positive exponent r, we have $p \,||\, Q_n$, where $n = \rho(p)p^r$, except when $p = 2$, $\rho(2) = 3$, and $r = 1$.*

Proof For any fixed $r \geq 1$, put $m = \rho(p)p^{r-1}$, and let $\rho(p) = p^s t$, where $p \nmid t$ and $s \geq 0$. We have $pm = p^{r+s} t\rho(p)$. From (4.28), we get

$$U_{pm}/U_m = \prod_{d|t} Q_{du},$$

where $u = p^{r+s}$. If $p \neq 2$, by Corollary 11, we have $p \,||\, U_{pm}/U_m$; thus, $p \,||\, Q_{ju}$ for some j such that $j \mid t$. By Lemma 24, we have $\rho(p) \mid ju$, and therefore $t \mid jp^r$, which since $p \nmid t$ means that $t \mid j$ and, since $j \mid t$, we get $t = j$. It follows that if $n = ju$, then $n = tu = \rho(p)p^r$ and $p \,||\, Q_n$. If $p = 2$, we can prove the lemma and the exception by using results derived in Sect. 2.5. □

Let $\mathrm{sqf}\,(n)$, sometimes called the *square-free kernel* of n, be the product of all the distinct primes which divide n. For example, $\mathrm{sqf}\,(360) = 2 \cdot 3 \cdot 5 = 30$. We are now able to prove the following lemma.

Lemma 26 *If $n \neq 1, 2,$ or 6, a sufficient condition that U_n contains at least one primitive divisor is that $|Q_n| > sqf(n)$.*

Proof We prove the contrapositive. If U_n contains no primitive divisors, then Q_n contains no primitive divisors. Thus, if any prime p divides Q_n, then p must divide some Q_m for some minimal m such that $0 < m < n$. It follows that by Lemma 24, we have $m = \rho(p)p^k$ for some $k \geq 0$ and $n = \rho(p)p^r$ for some $r \geq 0$. Since $n > m$, we must have $r \geq k + 1 \geq 1$. Thus, $p \mid n$, and by Lemma 25, we see that $p^2 \nmid Q_n$. Hence, Q_n divides $\operatorname{sqf}(n)$ and therefore $|Q_n| \leq \operatorname{sqf}(n)$. □

We now need to determine when the condition of $|Q_n| > \operatorname{sqf}(n)$ holds. We will assume that $n > 2$ is fixed in what follows. We observe that if ζ is a primitive nth root of unity, then

$$(\alpha - \zeta^k\beta)(\alpha - \zeta^{-k}\beta) = \alpha^2 + \beta^2 - \alpha\beta(\zeta^k + \zeta^{-k}) = P^2 - Q\theta_k$$

where $\theta_k = 2 + \zeta^k + \zeta^{-k} = 2 + 2\cos(2\pi k/n)$. Notice that if $\gcd(n, k) = 1$, then $0 < \theta_k < 4$. From (4.26) and the remarks following (4.28), we see that

$$Q_n = \prod (P^2 - Q\theta_k), \tag{4.30}$$

where the product is taken over all integers k such that $0 < k < n/2$ and $\gcd(n, k) = 1$.

Lemma 27 *If $D > 0$, then Q_n attains its least value when $P = 1$ and $Q = -1$ or when $P = 3$ and $Q = 2$.*

Proof Consider any fixed θ_k in (4.30). If $Q < 0$, then since we may assume $P \geq 1$, we get $P^2 - Q\theta_k \geq 1 + \theta_k$ with equality only when $P = 1$ and $Q = -1$. If $Q > 0$, then clearly $Q = 1$ or $Q > 1$. In the first case, because $D > 0$, we must have $P \geq 3$ and $P^2 - Q\theta_k \geq 0 - \theta_k > 9 - 2\theta_k > 0$. In the second case, we get

$$P^2 - Q\theta_k \geq 4Q + 1 - Q\theta_k = 9 - 2\theta_k + (Q - 2)(4 - \theta_k) \geq 9 - 2\theta_k$$

with equality holding only when $Q = 2$ and $P = 3$. The lemma now follows from (4.30). Thus, when $D > 0$, we need only check that $Q_n > \operatorname{sqf}(n)$ when U is either the Fibonacci sequence or the Mersenne sequence. □

In order to deal with these two possibilities, we make use of the lemma below:

Lemma 28 *If $n > 2$ and a is any real number such that $|a| < 1/2$, then $\Phi_n(a) \geq 1 - |a| - |a|^2$.*

Proof Since for any real x such that $|x| < 1$, we have $1 - x \geq 1 - |x|$ and $(1-x)^{-1} \geq 1-|x|$, it is clear that $(1-a^{n/d})^{\mu(d)} \geq 1-|a|^{n/d}$. By (4.25), we get

$\Phi_n(a) \geq \prod(1-|a|^i)$, where the product is taken over all positive integers i. Since for real x and y such that $0 < x, y < 1$, we have $(1-x)(1-y) \geq 1-x-y$, we find that

$$\Phi_n(a) \geq (1-|a|)(1-|a|^2-|a|^3-|a|^4-\cdots) = (1-|a|)(1-\frac{|a|^2}{1-|a|}) = 1-|a|-|a|^2.$$

We next deal with the Fibonacci case in the following lemma.

Lemma 29 *If $n \neq 1$, 2, 6, or 12, then for the Fibonacci sequence, we have $Q_n > sqf(n)$.*

Proof In this case, we put $\alpha = (1+\sqrt{5})/2 > 3/2$, $\beta = (1-\sqrt{5})/2$, and $|\beta/\alpha| = (3-\sqrt{5})/2 < 1/2$. By the previous lemma, we get $\Phi_n(\beta/\alpha) \geq 1-|\beta/\alpha|-|\beta/\alpha|^2 = 2\sqrt{5}-4 > 2/5$, and since $Q_n = Q_n(\alpha,\beta) = Q_n(\beta,\alpha) = \alpha^{\varphi(n)}\Phi_n(\beta/\alpha)$ by (4.27), we find that $Q_n > (2/5)(3/2)^{\varphi(n)}$. Thus, if

$$(2/5)(3/2)^{\varphi(n)} > \mathrm{sqf}\,(n), \tag{4.31}$$

we are done.

Let $\mathrm{sqf}\,(n) = q_1 q_2 \cdots q_t$, where the q_i $(i = 1, 2, \ldots, t)$ are distinct primes. Suppose $q_1^\nu \,||\, n$ and put $r = \varphi(q_1^\nu)$ and $m = n/q_1^\nu$; we note that $\varphi(n) = r\varphi(m)$. We will now show that if

$$(2/5)(3/2)^r > 2q_1, \tag{4.32}$$

then (4.31) holds. This is certainly the case for $m = 1$ or $m = 2$. Thus, we may now assume that $m \geq 3$; in this case, we have $\varphi(m) \geq 2$. We next observe that $2/5 > (2/5)^{\varphi(m)}$ and that

$$\frac{2}{5}\left(\frac{3}{2}\right)^{\varphi(n)} > \left(\frac{2}{5}\left(\frac{3}{2}\right)^r\right)^{\varphi(m)} > (2q_1)^{\varphi(m)} \geq q_1^2 2^{\varphi(m)} \geq q_1 2^{\varphi(u)+1}, \tag{4.33}$$

where $u = \mathrm{sqf}\,(n)/q_1$. If u is odd, then by Euler's theorem, we have $2^{\varphi(u)} \equiv 1 \pmod{u}$; consequently, $2^{\varphi(u)} > u$. If u is even, then $u/2$ is odd, and $2^{\varphi(u)} = 2^{\varphi(u/2)} \equiv 1 \pmod{u/2}$; hence, $2^{\varphi(u)+1} > u$. Since $u = \mathrm{sqf}\,(n)/q_1$, we can deduce (4.31) from (4.33).

Now, if k is any integer greater than 10, it is easy to show by induction that $(2/5)(3/2)^{k-1} > 2k$; thus, if q_1 is larger than 7, then (4.32) is true, and therefore, (4.31) holds. Also, if $q_1^\nu = 2^4$, 3^3, 5^2, 7^2, then (4.32) is true. Hence, (4.31) holds for higher powers of these primes. It remains, then, to consider only the cases of $n = 2^a 3^b 5^c 7^d$, where $0 \leq a \leq 3$, $0 \leq b \leq 2$, $0 \leq c \leq 1$, and $0 \leq d \leq 1$. By substituting these values of n into the left-hand side of (4.31), we find that the inequality (4.31) is true except for $n = 1$, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15, 18, 30. By direct computation of Q_n for each of these exceptional subscripts, we find that $Q_n > \mathrm{sqf}\,(n)$ for $n \neq 1$, 2, 3, 5, 6, 12. Since F_3 $(= 2)$ and F_5 $(= 5)$ each have a primitive divisor, we have our result. □

The following result can be proved for the Mersenne sequence.

Lemma 30 *If $n \neq 1$, 2, 6, then the nth term of the Mersenne sequence contains at least one primitive divisor.*

Proof In this case, we have $\alpha = 2$ and $\beta = 1$ and, by Lemma 28, $\Phi_n(\beta/\alpha) \geq 1/4$. It follows that $Q_n > (1/4)2^{\varphi(n)} > (2/5)(3/2)^{\varphi(n)}$, with the latter inequality holding for $n > 2$. The remainder of the proof follows by using reasoning similar to that employed in the proof of Lemma 29. □

We are finally able to prove Carmichael's theorem.

Theorem 64 (Carmichael [7]) *If $D > 0$ and $n \neq 1$, 2, 6, then U_n contains at least one primitive divisor except for $P = 1$, $Q = -1$, and $n = 12$.*

Proof By Lemma 27, we know that the least value of Q_n can only occur when $U_n = F_n$ or M_n. By Lemmas 29 and 30, we know that in these cases, we have $Q_n > \text{sqf}(n)$ when $n \neq 1$, 2, 3, 5, 6, 12. Thus, by Lemma 26, we see that U_n contains at least one primitive divisor when $n \neq 1$, 2, 3, 5, 6, 12. We compute $Q_5 = 5$ for F_n and $Q_5 = 31$ for M_n; hence, by Lemma 27, we have $Q_5 > 5$ when $U_n \neq F_n$. Also, if $U_n = F_n$, then 5 is a primitive divisor of $F_5 = 5$. Since $D > 0$, we have $Q < P^2/4$ and $Q_3 = P^2 - Q > 3P^2/4 > 3$ when $P > 1$. If $P = 1$ and $Q < -2$, we get $Q_3 > 3$, and if $P = 1$ and $Q = -2$, we get $Q_3 = 3$; in both cases, 3 is a primitive divisor of U_n. If $P = 1$ and $Q = -1$, we have the Fibonacci case, and 2 is a primitive divisor of F_3. There remains the case of $n = 12$. Since $Q_{12} = 13$ for the Mersenne numbers and $Q_{12} = 6$ for the Fibonacci numbers, we have $Q_{12} > 6$ when $U_n \neq F_n$. We have already seen that F_{12} does not contain a primitive divisor. □

In 1955, Ward [35] showed that a similar result holds for the Lehmer sequences $\bar{U}$.

Theorem 65 *If $D > 0$ and $n \neq 1$, 2, 6, then U_n contains at least one primitive divisor except for $R = 1$, $Q = -1$, and $n = 12$ or $R = 5$, $Q = 1$, and $n = 12$.*

Proof This can be shown by using reasoning similar to the above. An important observation is that if $n \neq 1$, 2, 6 and the cyclotomic number associated with $\bar{U}_n(R, Q)$ for both $R = 1$ and $Q = -1$ and $R = 5$ and $Q = 1$ is greater than $\text{sqf}(n)$, then all Lehmer sequences $\bar{U}_n$ contain at least one primitive divisor. □

As mentioned earlier, it is very difficult to find all the U_n and $\bar{U}_n$ which have primitive divisors in the case of $D < 0$. This problem was only completely solved relatively recently by Bilu et al. [2], where is it shown that for $n > 30$, any Lucas or Lehmer number must have a primitive divisor. This allowed the authors to present all U_n and $\bar{U}_n$, which do not have a primitive divisor. While [2] is the work of three authors, it must be emphasized that it

represents the culmination of many years of previous work by several investigators. As this material would take us well beyond the scope of this work, the interested reader should consult [2] for further information. This paper is very clearly written and contains an extensive bibliography.

4.6 Moduli for Which U Contains a Full Set of Residues

As in Sect. 4.1, let (X_n) denote any second-order linear recurrence with characteristic polynomial $x^2 - Px + Q$, where P and Q are integers such that $\gcd(P, Q) = 1$. Following Shah [28], we will say that a given positive integer m is *defective* with respect to (X_n) if a complete set of residues modulo m does not exist in (X_n); otherwise, we say that m is nondefective with respect to (X_n). For example, consider the Fibonacci sequence (F_n), where $F_n = U_n(1, -1)$. If we take this sequence modulo 5, we get $0, 1, 1, 2, 3, 0, 3, 3, 1, 4, \ldots$; thus, 5 is nondefective in (F_n) because a complete set of residues $\{0, 1, 2, 3, 4\}$ modulo 5 occurs in (F_n). Indeed, we have the more general result below.

Theorem 66 *Let p be any prime such that $p \mid D$, where $D = P^2 - 4Q$. If $U_n = U_n(P, Q)$, then p is nondefective with respect to (U_n).*

Proof If $p = 2$, then because $U_0 = 0$ and $U_1 = 1$, we see that p is nondefective with respect to (U_n); thus, we may now assume that p is odd. By (2.28), we have $U_m \equiv m(P/2)^{m-1} \pmod{p}$ for all $m \geq 0$. Also, since $p \mid D$ and $\gcd(P, Q) = 1$, we see that $p \nmid P$. If we let k be any integer such that $0 \leq k \leq p-1$ and put $m = p^2 - kp + k$, then $p - 1 \mid m - 1$, and for this value of m, we have

$$U_m \equiv k \pmod{p}.$$

It follows that (U_n) must contain a complete set of residues modulo p. □

On the other hand, if we take (F_n) modulo 8, we get the repeating sequence $0, 1, 1, 2, 3, 5, 0, 5, 5, 2, 7, 1, \ldots$ Since the residue 6 (mod 8) does not occur in this sequence, we see that 8 is defective in (F_n). With regard to the Fibonacci sequence (F_n), Burr [5] proved the theorem below.

Theorem 67 *The integer m is nondefective with respect to (F_n) if and only if $m = 5^k$, $2 \cdot 5^k$, $4 \cdot 5^k$, $3^j \cdot 5^k$, $6 \cdot 5^k$, $7 \cdot 5^k$, or $14 \cdot 5^k$, where $k \geq 0$ and $j \geq 1$.*

The purpose of this section is to investigate the question of when a given m can be nondefective in (X_n). The following simple result is essentially due to Shah.

Theorem 68 *If m is defective with respect to (X_n), then every positive multiple of m is also defective with respect to (X_n).*

Proof Suppose tm is not defective with respect to (X_n); then for every r where $0 \le r \le m-1$, there exists some X_n such that $X_n \equiv r \pmod{tm}$. Since $X_n \equiv r \pmod{m}$, we see that m is not defective, a contradiction. □

In what follows, we will assume that $\gcd(Q, m) = 1$; this, of course, is automatic when $|Q| = 1$. We have a somewhat surprising result mentioned in Somer and Křížek [33].

Theorem 69 *If m is nondefective with respect to (X_n), then m is nondefective with respect to (U_n).*

Proof By results in Sect. 4.1, we know that (X_n) is purely periodic modulo m; thus, we may assume with no loss of generality that $X_0 \equiv 0 \pmod{m}$. Put $d = \gcd(X_1, m)$, and note that since $d \mid X_0$, we must have $d \mid X_n$ for all $n \ge 0$ by the recursion for (X_n). If $d > 1$, then since $X_n \not\equiv 1 \pmod{m}$, we see that m is defective with respect to (X_n), a contradiction. Thus, $d = 1$ and $X_1 \equiv c \pmod{m}$, where $\gcd(c, m) = 1$. Once again, by the recursion for (X_n), we find that

$$U_n \equiv c^{-1} X_n \pmod{m},$$

for all $n > 0$, where $c^{-1}c \equiv 1 \pmod{m}$. Thus, m is also nondefective with respect to (U_n). □

In view of Theorems 68 and 69, we see that it is important to examine the question of whether a prime p can be nondefective in (U_n).

Theorem 70 *If p is any odd prime such that the Legendre symbol $(D \mid p) = 1$, then p is defective with respect to (U_n).*

Proof By Lemma 9 and Theorem 9, we have $U_p \equiv 1$ and $U_{p-1} \equiv 0 \pmod{p}$. It follows from the recurrence (2.1) that

$$U_{p-1+n} \equiv U_n \pmod{p} \quad (n \ge 0).$$

Thus, the period length τ of (U_n) must be such that $\tau \le p-1$. Since there can be at most $p-1$ $(< p)$ distinct elements in the periodic part of (U_n) modulo p, we see that p must be defective with respect to (U_n). □

The situation when $(D \mid p) = -1$ is more complicated. We know that in this case (Lemma 9 and Theorem 9), we have $U_p \equiv -1$, $U_{p+1} \equiv 0$, and therefore $U_{p+2} \equiv Q \pmod{p}$. We also have the easily verified (by simply using the formula for U_n in (2.5)) Lucas sequence identities

$$U_{n+m} = U_{n+1}U_m - QU_nU_{m-1} \quad (n \ge 0,\ m \ge 1), \quad \text{and}$$
$$Q^m U_{n-m} = U_nU_{m+1} - U_{n+1}U_m \quad (n \ge m \ge 0).$$

Both of these identities are special cases of the more general

$$U_kU_{n+m} = U_nU_{m+k} - Q^kU_mU_{n-k},$$

given as (4.2.14) in Williams [39]. Putting $n = p$ and $m = r + 1$ in the first of these yields

$$U_{p+1+r} \equiv QU_r \pmod{p} \quad (r \geq 0) \tag{4.34}$$

and putting $n = p + 1$, $m = r$ in the second yields

$$Q^r U_{p+1-r} \equiv -QU_r \pmod{p} \quad (r \geq 0). \tag{4.35}$$

By iterating (4.34), we get

$$U_{k(p+1)+r} \equiv Q^k U_r \pmod{p} \quad (k \geq 0,\ r \geq 0), \tag{4.36}$$

and by using (4.36) together with (4.35), we find that

$$U_{k(p+1)-r} \equiv -Q^{k-r} U_r \pmod{p} \quad (k \geq 1,\ r \geq 0). \tag{4.37}$$

From these two results, we see that for $r = 1$,

$$U_{k(p+1)+1} \equiv Q^k,\ U_{(k+1)(p+1)-r} \equiv -Q^k \pmod{p} \quad (k \geq 0). \tag{4.38}$$

Theorem 71 *Suppose that p is an odd prime and $(D \mid p) = -1$. If Q belongs to the exponent $p-1 \pmod{p}$, then p is nondefective with respect to (U_n); if Q belongs to the exponent $(p-1)/2 \pmod{p}$ and $p \equiv -1 \pmod{4}$, then p is also nondefective with respect to (U_n).*

Proof If Q belongs to the exponent $p-1$ modulo p, then Q is a primitive root modulo p. By the first result in (4.38) and $U_0 = 0$, we see that (U_n) contains a complete set of residues modulo p. If Q belongs to the exponent $(p-1)/2 \pmod{p}$ and $p \equiv -1 \pmod{4}$, then no power of Q can be -1 modulo p. Hence, by both results in (4.38), we see that (U_n) must contain a complete set of residues modulo p. □

Now suppose p is a prime such that $p = 2q + 1$, where q is an odd prime. Such primes are called *Sophie Germain primes*, and it is widely believed by analytic number theorists (but not yet proved) that there exists an infinitude of such primes. Indeed, if $P(x)$ denotes the number of Sophie Germain primes $< x$, then it follows by Hypothesis H of Bateman and Horn [1] that $P(x) \sim 2Cx/(\log x)^2$, where $C = 0.6601618\cdots$, and it has been shown that this estimate is quite accurate for x up to 10^{10}. (See Sect. 3.5 of Caldwell [6].) For such a prime p, we see that if $p \nmid Q$ and $|Q| \neq 1$, then Q belongs to the exponent $p-1$ or $(p-1)/2 \pmod{p}$. Also, by a result like Theorem 5.3.1 of [39], we know that for each value of Q, there exist precisely $(p - (Q \mid p))/2$ values of P modulo p such that $((P^2 - 4Q) \mid p) = (D \mid p) = -1$. Thus, by Theorem 4.4.6, there must exist many pairs (P, Q) modulo p such that any Sophie Germain prime p is nondefective with respect to the corresponding (U_n). As a consequence of this, it is very likely that if $|Q| > 1$, then there

exist infinitely many primes p such that p is nondefective in some (U_n). This strongly suggests that the problem of determining all nondefective primes with respect to a given (U_n) becomes extremely difficult to manage when $|Q| \neq 1$. It is for this reason that we assume that $|Q| = 1$ in the sequel. We now deal with the case of an odd prime p such that $(D \,|\, p) = -1$ and $Q = 1$.

Theorem 72 *If $p \geq 5$ is a prime such that $(D \,|\, p) = -1$ and $Q = 1$, then p is defective with respect to (U_n).*

Proof By (4.34), we have $U_{p+1+n} \equiv U_n \pmod{p}$ $(n \geq 0)$. Thus, (U_n) is periodic modulo p with period length $p + 1$. Put $r = (p + 1)/2$, and observe from Theorem 36 that p divides U_r. From (2.10) with $m = r$, we get

$$2U_{n+r} \equiv U_n V_r \pmod{p};$$

also, from (2.8), we have $V_r^2 \equiv 4 \pmod{p}$. Thus, $V_r \equiv 2\eta \pmod{p}$ and

$$U_{r+n} \equiv \eta U_n \pmod{p}, \tag{4.39}$$

where η is either 1 or -1 and fixed. We also see from (2.10) that

$$2U_n = 2U_{n-r+r} \equiv U_{n-r}V_r \equiv 2\eta U_{n-r} \pmod{p}.$$

By (2.7), we have

$$U_n \equiv -\eta U_{r-n} \pmod{p}. \tag{4.40}$$

It follows from (4.39) and (4.40) that the only possible distinct terms in the period of $(U_n) \pmod{p}$ can be

$$0, \ \pm U_1, \ \pm U_2, \ \ldots, \pm U_s,$$

where $s = \lfloor r/2 \rfloor$. Since $2s + 1 \leq r + 1 < p$ $(p > 3)$, we see that p must be defective with respect to (U_n). □

In the case of $(D \,|\, p) = -1$ and $Q = -1$, we have the following result.

Theorem 73 *If $p \geq 11$ is a prime such that $(D \,|\, p) = -1$ and $Q = -1$, then p is defective with respect to (U_n).*

This result was partially demonstrated by Somer [31] and completely proved by Schinzel [27], using a different technique. Later, Li [13] established this result by extending Somer's methods.

Now that all the possible primes that are nondefective in (U_n) can be easily identified, it is feasible to extend Theorem 67 to include all sequences (U_n) with $|Q| = 1$. This was done in exhaustive detail by Somer and Křížek [32]. As the results in [32] are quite lengthy and detailed, we refer the interested reader to that paper for further information and references.

References

1. P. Bateman and R. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comp. **16** (1962), 363–367.
2. Y. Bilu, G. Hanrot and P. Voutier, *The existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math. **539** (2001), 75–122.
3. G. Brandner, *RSA, Dickson, LUC and Williams: a study on four polynomial-type public-key cryptosystems*, Applicable Algebra in Engineering Communication and Computing **24** (2013), 17–36.
4. J. Brillhart, P. L. Montgomery, and R. D. Silverman, *Tables of Fibonacci and Lucas factorizations*, Math. Comp. **50** (1988), 251–260.
5. S. Burr, *On moduli for which the Fibonacci sequence contains a complete system of residues*, Fibonacci Quart. **9** (1971), 497–504.
6. C. Caldwell, *An Amazing Prime Heuristic*, https://arxiv.org/abs/2103.04483
7. R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Annals of Math. **15** (1913), 30–70.
8. Richard Crandall and Carl Pomerance, *Prime Numbers: A Computational Perspective*, Springer-Verlag, New York, 2001.
9. A. Granville and P. Pleasants, *Aurifeuillian factorization*, Math. Comp. **75** (2005), 497–508.
10. Dov Jarden, *Recurring Sequences*, 2nd ed., Riveon Lematematika, 1966.
11. L. Kocarev, J. Makraduli and P. Amato, *Public-key encryption based on Chebyshev polynomials*, Circuits, Systems and Signal Processing **24** (2005), 497–517.
12. D. H. Lehmer, *An extended theory of Lucas' functions*, Annals of Math. **31** (1930), 419–448.
13. H.-C. Li, *Complete and reduced systems of second-order recurrences modulo p*, Fibonacci Quart. **38** (2000), 272–281.
14. R. Lidl and H. Niederreiter, *Finite Fields*, Adison-Wesley, Reading, MA, 1983.
15. R. Lidl, G. L. Mullen and G. Turnwald, *Dickson Polynomials*, Longman Scientific and Technical, NY, 1993.
16. É. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. of Math. **1** (1878), 184–240, 289–321.
17. É. Lucas, *Théorème d'arithmétique*, Atti della Reale Accademia delle scienze di Torino **13** (1878), 271–278.
18. É. Lucas, *Sur les formules de Cauchy et de Lejeune-Dirichlet*, Assoc. Française pour l'Avancement des Sciences, Comptes Rendus **7** (1878), 164–173.
19. J. C. Mason and D. C. Handscomb, *Chebyshev Polynomials*, Chapman&Hall/CRC, Boca Raton, FL, 2003.
20. R. McIntosh and M. Dipra, *Carmichael numbers with* $p+1 \mid n+1$, J. of Number Theory **147** (2015), 81–91.

21. G. Mullen and D. Panario, *Handbook of Finite Fields*, CRC Press, Boca Raton FL, 2013.
22. W. B. Müller and W. Nöbauer, *Some remarks on public-key cryptosystems*, Studia Sci. Math. Hungar. **16** (1981), 71–76.
23. R. Pinch, *Absolute quadratic pseudoprimes*, Proc. Conf. Algorithmic Number Theory 2007, Turku Centre for Computer Science General Publication **46** 2007, 113–128.
24. R. Pinch, *The Carmichael numbers up to* 10^{21}, Proc. Conf. Algorithmic Number Theory 2007, Turku Centre for Computer Science General Publication **46** (2007), 129–131.
25. Hans Riesel, *Prime Numbers and Computer Methods for Factorization*, 2nd Edition, Birkhäuser, Boston, 1994.
26. E. Roettger and H. Williams, *Generalized Jarden's Theorem*, J. Integer Seq. **25** (2022), Art. 22.7.2.
27. A. Schinzel, *Special Lucas sequences, including the Fibonacci sequence, modulo a prime*, A Tribute to Paul Erdős, Cambridge Univ. Press, Cambridge, 1990, 349–357.
28. A. Shah, *Fibonacci sequence modulo m*, Fibonacci Quart. **6** (1968), 139–141.
29. A. Shallue and J. Webster, *Fast tabulation of challenge pseudoprimes*, 13th Algorithmic Number Theory Symposium, 411–423, Springer, NY, 2019.
30. Harold Shapiro, *Introduction to the Theory of Numbers*, Wiley-Interscience, NY, 1983.
31. L. Somer, *Primes having incomplete residue systems for a class of second order recurrences*, Applications of Fibonacci Numbers, Vol.2, Kluwer Academic Publ, Dordrecht, 1988, 113–141.
32. L. Somer and M. Křížek, *On moduli for which certain second-order linear recurrences contain a complete system of residues modulo m*, Fibonacci Quart. **55** (2017), no. 3, 209–228.
33. L. Somer and M. Křížek, *Nondefective integers with respect to certain Lucas sequences of the second kind*, Integers, **18** (2018),#A35.
34. S. S. Wagstaff, Jr., *The Joy of Factoring*, Volume **68** *Student Mathematical Library*, American Mathematical Society, Providence, RI, 2013.
35. M. Ward, *The intrinsic divisors of Lehmer numbers*, Annals of Math. **62** (1955), 230–236.
36. J. Webster and A. Gurovski, private communication, 2016.
37. S. Weintraub, *Several proofs of the irreducibility of the cyclotomic polynomials*, American Mathematical Monthly **120** (2013), 537–545.
38. H. C. Williams, *On numbers analogous to Carmichael numbers*, Canad. Math. Bull. **28** (1977), 133–143.
39. H. C. Williams, *Édouard Lucas and Primality Testing*, Canadian Math. Soc. Series of Monographs and Advanced Texts, John Wiley and Sons, NY, 1998.

40. R. Wituła and D. Słota, *On modified Chebyshev polynomials*, J. Math. Anal. Appl. **324** (2006), 321–343.
41. M. Yabuta, *A simple proof of Carmichael's theorem on primitive divisors*, Fibonacci Quart. **39** (2001), 439–443.

Chapter 5
Some Properties of Lucasnomials

Quand on sait dire, on peut tout faire. (Marcel Proust)

Lorsque les connaissances sont un amas d'erreurs et de vérités, indistinctement mêlées ; lorsqu'une longue ignorance et beaucoup de siècles leur ont laissé jeter des racines profondes, la séparation en est difficile. L'ancienneté ne prouve rien. Le respect, la croyance de plusieurs âges ne sont que des préjugés. (Sophie Germain)

Abstract Lucasnomials, or Lucasnomial coefficients, are a generalization of the usual binomial coefficients $\binom{n}{k}$, when n and k are integers. Lucasnomials $\binom{n}{k}_U$ are associated with every nondegenerate fundamental Lucas sequence U. Their definition includes ordinary binomial coefficients which we get when $U = U(2, 1)$, i.e., if U is the sequence of natural numbers. Remarkably, various arithmetic properties of binomial coefficients hold in a more general form in this context.

5.1 Definition. Connection with q-Binomial Coefficients

Definition 5 (Lucasnomials) Suppose $U = U(P, Q)$ is a nondegenerate fundamental Lucas sequence. Assume n and k are integers. We define the Lucasnomial, or Lucasnomial coefficient $\binom{n}{k}_U$, as follows.

$$\binom{n}{k}_U = \begin{cases} \frac{U_n U_{n-1} \cdots U_{n-k+1}}{U_k U_{k-1} \cdots U_1}, & \text{if } k \geq 1; \\ 1, & \text{if } k = 0; \\ 0, & \text{if } k < 0. \end{cases} \tag{5.1}$$

As we will see in the next section, Lucasnomials are always integers if $n \geq 0$. Lucasnomials are called *Fibonomials* if U is the Fibonacci sequence, that is, if $U = U(1, -1)$. A number of properties of general Lucasnomials were first hinted at through studies of Fibonomials.

© Springer Nature Switzerland AG 2023

C. J.-C. Ballot, H. C. Williams, *The Lucas Sequences*, CMS/CAIMS Books in Mathematics 8, https://doi.org/10.1007/978-3-031-37238-4_5

We point out here the close connection between q-binomial coefficients or Gaussian coefficients, introduced by Gauss, and Lucasnomials. Formally, Gaussian coefficients $\binom{n}{k}_q$ are defined by replacing any term U_i, $i \geq 0$, in Equation (5.1) by the q-number

$$i_q := 1 + q + q^2 + \cdots + q^{i-1} = \frac{q^i - 1}{q - 1} = U_i(q + 1, q). \tag{5.2}$$

The q-binomial coefficients are defined as rational functions in the variable q, which actually turn out to be polynomials in $\mathbb{Z}[q]$. If we assign and fix an integer value for q, with $|q| \geq 2$, then, by Definition 5, they become Lucasnomials with respect to the sequence $U(q + 1, q)$. Gaussian coefficients turn up in various mathematical areas and have also been the object of study of many articles. Their properties also generalize properties of binomial coefficients. By letting the variable q tend to 1 in an identity involving Gaussian coefficients, we often either recover or discover an identity satisfied by binomial coefficients. But it is also possible to obtain a Lucasnomial identity from an identity for q-binomial coefficients directly, and vice versa. The upshot is that there are two main roads to the study of Lucasnomials. One uses Lucas sequences and their arithmetic properties, or particular Lucas sequences such as the Fibonacci sequence, while the other main source comes from q-calculus.

To convert a q-identity into a Lucasnomial identity, where $U = U(P, Q)$, α and β are the zeros of $x^2 - Px + Q$, or vice versa, one may use the transformation formulas

$$q = \frac{\alpha}{\beta} = Q\beta^{-2}, \tag{5.3}$$

and

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \beta^{n-1}\frac{q^n - 1}{q - 1}, \tag{5.4}$$

and, therefore,

$$\binom{n}{k}_U = \beta^{\sum_{i=1}^{k}((n-i)-(i-1))}\binom{n}{k}_q = \beta^{k(n-k)}\binom{n}{k}_q. \tag{5.5}$$

Example 74 Consider for $n \geq k \geq 0$ the q-identity

$$\binom{n}{k}_q = q^k\binom{n-1}{k}_q + \binom{n-1}{k-1}_q, \tag{5.6}$$

which has elegant combinatorial proofs, but is easy to check algebraically. Using (5.3) and (5.5), we see that

$$\beta^{-k(n-k)}\binom{n}{k}_U = Q^k\beta^{-2k}\beta^{-k(n-1-k)}\binom{n-1}{k}_U + \beta^{-(k-1)(n-k)}\binom{n-1}{k-1}_U.$$

Multiplying by $\beta^{k(n-k)}$ and using $Q = \alpha\beta$, we obtain the Lucasnomial identity

$$\binom{n}{k}_U = \alpha^k \binom{n-1}{k}_U + \beta^{n-k} \binom{n-1}{k-1}_U. \tag{5.7}$$

Occasionally, it may also be worth viewing Lucasnomials as polynomials in $\mathbb{Z}[P, Q]$, a result we will establish in the next section.

5.2 Integrality

Lucas [56, p. 203] stated that the product of any n consecutive terms of a sequence U is divisible by its first n terms, with a near-complete justification. If, say, binomial coefficients are introduced via their factorial formula, then one may prove their integrality using the Pascal identity (5.19) and an induction argument. This is, in fact, how Lucas justifies his statement [56, p. 203] after giving a simple proof of the generalized Pascal identity (5.20). Many proofs of the integrality of Lucasnomials in the more recent literature actually follow this path. Ward [79] proved that generalized binomial coefficients (see Definition 6) with respect to a strong divisible[†] sequence $X = (x_n)_{n\geq 0}$ are integers. Hence, his result implies the integrality of Lucasnomials when $\gcd(P, Q) = 1$. Combinatorial interpretations of Lucasnomials are, among other means, yet other proofs of their integrality. We will mention these in Sect. 5.4. By viewing Lucasnomials as rational functions in P and Q, we will prove them to be polynomials in $\mathbb{Z}[P, Q]$ using a remark made in the proof of [71, Prop. 2]. That they are integers immediately follows.

Note that, by (2.31), for a pair of integers P and Q, $U_n(P, Q)$ is the value of the polynomial $\Psi_n(P, Q)$ in $\mathbb{Z}[P, Q]$ for all $n \geq 0$. By (2.32) or (2.34), we also see that $V_n(P, Q)$ is a polynomial in $\mathbb{Z}[P, Q]$.

Definition 6 (Generalized binomial coefficients) Suppose $X = (x_n)_{n\geq 0}$ or $(x_n)_{n\in\mathbb{Z}}$ is a sequence of complex numbers, polynomials, or functions with $x_0 = 0$ and $x_n \neq 0$ $(n > 0)$. We define the generalized binomial coefficient with respect to X for all $n \geq 0$ or all $n \in \mathbb{Z}$, as the case may be, as follows:

$$\binom{n}{k}_X = \begin{cases} \frac{x_n x_{n-1} \cdots x_{n-k+1}}{x_k x_{k-1} \cdots x_1}, & \text{if } k \geq 1; \\ 1, & \text{if } k = 0; \\ 0, & \text{if } k < 0. \end{cases} \tag{5.8}$$

Remark 24 Lucas did not formally define Lucasnomials. An abstract general definition, such as Definition 6, appears in a 1915 one-page note of Fontené [28]. However, Ward's 1936 paper [80] might have been the first paper to

[†] That is, a strong divisibility sequence as is more traditional to say.

develop properties of generalized binomial coefficients with respect to an abstract sequence of complex numbers $X = (x_n)_{n\geq 0}$ satisfying $x_0 = 0$, $x_1 = 1$, and $x_n \neq 0$ for $n \geq 2$. He uses the pretty terminology "binomial coefficient to the base X."

Lemma 31 *Suppose $X = (x_n)_{n\geq 0}$ or $(x_n)_{n\in\mathbb{Z}}$ is a sequence of nonzero complex numbers or functions except that $x_0 = 0$. If $k \geq 1$ and n are integers and*

$$rx_n = sx_{n-k} + tx_k, \tag{5.9}$$

where r, s, and t are variables, or complex numbers or functions, then

$$r\binom{n}{k}_X = s\binom{n-1}{k}_X + t\binom{n-1}{k-1}_X. \tag{5.10}$$

Proof Indeed,

$$\begin{aligned} r\binom{n}{k}_X &= r\frac{x_n}{x_k}\binom{n-1}{k-1}_X \\ &= \frac{sx_{n-k} + tx_k}{x_k}\binom{n-1}{k-1}_X \\ &= s\frac{x_{n-k}}{x_k}\binom{n-1}{k-1}_X + t\binom{n-1}{k-1}_X \\ &= s\binom{n-1}{k}_X + t\binom{n-1}{k-1}_X. \end{aligned}$$

Definition 7 If n and k are integers, $n \geq 0$, then the Lucaspolynomial $\binom{n}{k}_\Psi$ is the generalized binomial coefficient with respect to the sequence of polynomials $(\Psi_n)_{n\geq 0}$ defined in (2.31).

We need a small lemma to convert some Lucas identities into polynomial identities.

Lemma 32 *If two complex-coefficient polynomials in two variables $f(P, Q)$ and $g(P, Q)$ are equal for all nonzero integer values of P and Q, then $f = g$.*

Proof We may fix the variable Q and obtain two polynomials f_Q and g_Q in P which, being equal for infinitely many values of P, must be identical. The coefficients of f_Q and g_Q are polynomials in Q which are equal for infinitely many values of Q. Hence, these polynomial coefficients are identical on both sides. Thus, $f = g$ as polynomials in P and Q. □

For an example, the identity (2.42)

$$U_m = U_{n+1}U_{m-n} - QU_{m-n-1}U_n,$$

valid for all Lucas sequences U, holds for all nonzero values of P and Q. Both sides of the equation can be viewed as polynomials in P and Q. Therefore, by Lemma 32, we see that

$$\Psi_m = \Psi_{n+1}\Psi_{m-n} - Q\Psi_{m-n-1}\Psi_n. \tag{5.11}$$

Theorem 75 *Suppose $n \geq k \geq 1$ are integers. Then the Lucaspolynomial $\binom{n}{k}_\Psi$ is a polynomial in P and Q with integer coefficients.*

Proof We saw just in (5.11) that

$$\Psi_n = \Psi_{k+1}\Psi_{n-k} - Q\Psi_{n-k-1}\Psi_k.$$

By Lemma 31 with $r = 1$, $s = \Psi_{k+1}$, and $t = -Q\Psi_{n-k-1}$, we obtain the identity

$$\binom{n}{k}_\Psi = \Psi_{k+1}\binom{n-1}{k}_\Psi - Q\Psi_{n-k-1}\binom{n-1}{k-1}_\Psi. \tag{5.12}$$

That $\binom{n}{k}_\Psi$ is in $\mathbb{Z}[P, Q]$ follows by the verification of the initial values and induction on n. □

Corollary 76 If $U(P, Q)$ is a nondegenerate fundamental Lucas sequence and $n \geq 0$ and k are integers, then $\binom{n}{k}_U$ is an integer. □

Proof Note that the nondegeneracy of U makes Lucasnomials well defined. If $k < 0$, then $\binom{n}{k}_U = 0$. If $k = 0$, then $\binom{n}{k}_U = 1$. So we may assume $k \geq 1$. If $0 \leq n < k$, then, since $U_0 = 0$, $\binom{n}{k}_U = 0$. Assume $n \geq k \geq 1$. Theorem 75 implies that $\binom{n}{k}_U$ is an integer. □

We now state a useful corollary to Lemma 31.

Corollary 77 Suppose $X = (x_n)_{n\in\mathbb{Z}}$ is a sequence of complex numbers or functions with $x_n = 0$ if and only if $n = 0$. Assume for all n and k

$$rx_n = sx_{n-k} + tx_k,$$

where r, s, and t are functions of n and k such that $r = s$ if $n = k = 0$. Then Equation (5.10), i.e.,

$$r\binom{n}{k}_X = s\binom{n-1}{k}_X + t\binom{n-1}{k-1}_X,$$

holds for all integers n and k. □

Proof This follows from Lemma 31 for all integers n if $k \geq 1$. If $k < 0$, then both sides of (5.10) are null. If $k = 0$, then (5.10) holds if and only if $r = s$. By hypothesis, $rx_n = sx_n + tx_0 = sx_n$. If $n \neq 0$, then $x_n \neq 0$ and so $r = s$. If $k = 0$ and $n = 0$, then $r = s$ by hypothesis. Thus, (5.10) holds in all cases. □

Corollary 78 Suppose $U(P,Q)$ is a nondegenerate fundamental Lucas sequence and n and k are integers. Then

$$\binom{n}{k}_U = U_{k+1}\binom{n-1}{k}_U - QU_{n-k-1}\binom{n-1}{k-1}_U. \tag{5.13}$$

Proof The corollary follows from the polynomial identity (5.12) for $n \geq k \geq 1$. But applying Corollary 77 to the Lucas identity $U_n = U_{k+1}U_{n-k} - QU_{n-k-1}U_k$ with $X = U$, $r = 1$, $s = U_{k+1}$, and $t = -QU_{n-k-1}$ yields the full result. □

Unfortunately, identity (5.13) is not a direct generalization of the addition property $\binom{m}{n} = \binom{m-1}{n} + \binom{m-1}{n-1}$ of binomial coefficients. Such generalizations exist. Indeed, identity (5.7) is one of them. But we will present some others in the next subsection.

5.3 Ten Basic Identities

In [33, p. 174], ten basic essential properties of binomial coefficients $\binom{r}{k}$, r complex, k integral, are listed. We borrow the names of these properties from the book [33] and present their extension to Lucasnomials. Since we did not attempt to generalize Lucasnomials for r complex or real, we take r to be an integer n. We assume U to be a nondegenerate fundamental Lucas sequence. Putting $P = 2$ and $Q = 1$ yields the corresponding binomial identity since for all integers n, $U_n(2,1) = n$. Note that $V_n(2,1) = 2$ for all n.

1. Factorial expansion. For $1 \leq k \leq n$ integers, the formula

$$\binom{n}{k}_U = \frac{U_nU_{n-1}\cdots U_1}{(U_k\cdots U_1)(U_{n-k}\cdots U_1)} \tag{5.14}$$

is obtained by multiplying numerator and denominator in Definition 5 by $U_{n-k}\cdots U_1$.

2. Symmetry. For all integers $n \geq 0$, we find that

$$\binom{n}{k}_U = \binom{n}{n-k}_U. \tag{5.15}$$

If $k < 0$, then $n - k > 0$ and $U_nU_{n-1}\cdots U_{n-(n-k)+1} = U_nU_{n-1}\cdots U_{k+1} = 0$ and both sides of (5.15) are zero. Both sides are 1 for $k = 0$. The identity holds for $k \geq 1$ by (5.14) since $n - (n-k) = k$.

3. Absorption. For k nonzero and from Definition 5, we find that

$$\binom{n}{k}_U = \frac{U_n}{U_k}\binom{n-1}{k-1}_U. \tag{5.16}$$

4. Upper negation. The formula

$$\binom{n}{k}_U = (-1)^k Q^{kn-\frac{k(k-1)}{2}} \binom{k-n-1}{k}_U \tag{5.17}$$

holds for all integers n and k.

Proof If $k = 0$, then both sides of the formula are 1. If $k < 0$, then both sides are 0. Assume $k \geq 1$. Since $\sum_{i=0}^{k-1}(n-i) = kn - \frac{k(k-1)}{2}$ and, by (2.7), $Q^j U_{-j} = -U_j$, we see that

$$\begin{aligned} Q^{kn-\frac{k(k-1)}{2}} \binom{k-n-1}{k}_U &= \frac{(Q^{n-(k-1)}U_{k-n-1})(Q^{n-(k-2)}U_{k-n-2})\cdots(Q^n U_{-n})}{U_k \cdots U_1} \\ &= (-1)^k \frac{U_n U_{n-1} \cdots U_{n-k+1}}{U_k \cdots U_1} \\ &= (-1)^k \binom{n}{k}_U. \end{aligned}$$

5. Trinomial revision. The identity

$$\binom{m}{n}_U \binom{n}{k}_U = \binom{m}{k}_U \binom{m-k}{n-k}_U \tag{5.18}$$

holds for all integers m, n, and k.

Proof If $k < 0$, then both sides are 0. Both sides are $\binom{m}{n}_U$ if $k = 0$. So we assume $k \geq 1$. Again, both sides are equal if $n \leq k$, whether $n < 0$, $0 \leq n < k$, or $n = k$. Thus, now suppose $n > k \geq 1$. For all integers m, we may write

$$\begin{aligned} \binom{m}{k}_U \binom{m-k}{n-k}_U &= \frac{U_m U_{m-1} \cdots U_{m-k+1}}{U_k \cdots U_1} \cdot \frac{U_{m-k} \cdots U_{m-n+1}}{U_{n-k} \cdots U_1} \\ &= \frac{U_m U_{m-1} \cdots U_{m-n+1}}{(U_k \cdots U_1)(U_{n-k} \cdots U_1)} \cdot \frac{U_n \cdots U_{n-k+1}}{U_n \cdots U_{n-k+1}} \\ &= \frac{U_m U_{m-1} \cdots U_{m-n+1}}{U_n \cdots U_1} \cdot \frac{U_n \cdots U_{n-k+1}}{U_k \cdots U_1} \\ &= \binom{m}{n}_U \binom{n}{k}_U. \end{aligned}$$

Remark 25 As noted by Gould [34, p. 26], the identity (5.18) holds for any generalized binomial coefficients in the sense of Definition 6.

6. Addition/Induction. The identity

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}, \tag{5.19}$$

sometimes called, particularly in countries influenced by French culture, the Pascal identity, has the direct extension

$$\binom{n}{k}_U = \frac{V_k}{2}\binom{n-1}{k}_U + \frac{V_{n-k}}{2}\binom{n-1}{k-1}_U, \tag{5.20}$$

which holds for all integers n and k.

Proof If $k < 0$, then both sides are 0. If $k = 0$, then both sides are equal to 1 since $V_0 = 2$. Thus, we assume $k \geq 1$. Applying Lemma 31 with the Lucas identity (2.10), written in the shape $2U_n = V_k U_{n-k} + V_{n-k}U_k$, where $r = 2$, $s = V_k$, and $t = V_{n-k}$, we obtain Equation (5.20) after division by 2. □

Remark 26 Another direct extension of Pascal's identity was given in (5.7) since $\alpha = \beta = 1$ for $U(2, 1)$. Actually, identity (5.7) is valid if we interchange the roles of the zeros α and β. Thus, adding (5.7) to its conjugate identity

$$\binom{n}{k}_U = \beta^k\binom{n-1}{k}_U + \alpha^{n-k}\binom{n-1}{k-1}_U \tag{5.21}$$

yields a second proof of (5.20). Note that we got (5.7) from the q-identity (5.6). However, we can derive (5.7) from Corollary 77 and the identity $U_n = \alpha^k U_{n-k} + \beta^{n-k}U_k$. The same holds true of the q-identity (5.6), since $q^n - 1 = q^k(q^{n-k}-1)+q^k-1$ implies that $n_q = q^k(n-k)_q + k_q$. Finally, we observe that, by Corollary 77, (5.7) is true for all integers n and k, not just for $n \geq k \geq 0$.

Remark 27 It is interesting to note that if one applies (5.20) to the Lucasnomial $\binom{k-n-1}{k}_U$, where $k \geq 1$, multiply the equation that results by $(-1)^k Q^{kn-\frac{k(k-1)}{2}}$ and perform upper negation on all three Lucasnomials, then, after some simplification, one obtains

$$2Q^k\binom{n}{k}_U = V_k\binom{n+1}{k}_U - V_{n+1}\binom{n}{k-1}_U.$$

Up to an index shift, the preceding equation follows from applying Lemma 31 to identity (2.12), written in the form $V_k U_n = 2Q^k U_{n-k} + V_n U_k$. In fact, the identity (5.22) is as much a direct extension of the usual addition of binomial coefficients as the identity (5.20). Thus, we record it below. The equation

$$V_k\binom{n}{k}_U = 2Q^k\binom{n-1}{k}_U + V_n\binom{n-1}{k-1}_U \tag{5.22}$$

holds for all integers n and k.

7. Upper summation. The summation on the upper index

$$\sum_{0\leq i\leq n}\binom{i}{k} = \binom{n+1}{k+1}$$

derives naturally from the Pascal identity. It was noted by Gould [34, eq. (13)] that for generic generalized binomial coefficients with respect to some $X = (x_n)_{n\geq 0}$, we have the general formula

$$\sum_{0\leq i\leq n} \frac{x_i - x_{i-k}}{x_k} \binom{i}{k}_X = \binom{n+1}{k+1}_X.$$

Now since we have several Lucasnomial generalizations of the Pascal identity, we obtain several corresponding generalizations for the upper summation formula. One comes from identity (5.7):

$$\sum_{0\leq i\leq n} \alpha^{(n-i)(k+1)}\beta^{i-k} \binom{i}{k}_U = \binom{n+1}{k+1}_U, \tag{5.23}$$

which holds for all nonnegative integers n and k.

Proof Fix $k \geq 0$ to an arbitrary value, and perform an induction on $n \geq 0$. Then express $\binom{n+2}{k+1}_U$ as $\alpha^{k+1}\binom{n+1}{k+1}_U + \beta^{n+1-k}\binom{n+1}{k}_U$ using identity (5.7), and we readily obtain, using the inductive hypothesis, that $\binom{n+2}{k+1}_U$ equals

$$\sum_{0\leq i\leq n+1} \alpha^{(n+1-i)(k+1)}\beta^{i-k} \binom{i}{k}_U.$$

Similar inductive proofs yield, for all nonnegative n and k, the generalizations

$$\sum_{0\leq i\leq n} 2^{i-n-1} V_{k+1}^{n-i} V_{i-k} \binom{i}{k}_U = \binom{n+1}{k+1}_U \tag{5.24}$$

and

$$\sum_{0\leq i\leq n} (2Q^{k+1})^{n-i} V_{k+1}^{i-k-1} V_{i+1} \binom{i}{k}_U = V_{k+1}^{n-k} \binom{n+1}{k+1}_U, \tag{5.25}$$

using, respectively, the generalized Pascal identities (5.20) and (5.22).

8. Parallel summation. Parallel summation

$$\sum_{i\leq k} \binom{n+i}{i} = \binom{n+k+1}{k}$$

also derives naturally from the Pascal identity. Using one of the three generalizations (5.7), (5.20), or (5.22) of the addition/induction formula, we obtain three respective generalizations of parallel summation, which are

$$\sum_{i\leq k} \alpha^i (\beta^{n+1})^{k-i} \binom{n+i}{i}_U = \binom{n+k+1}{k}_U, \tag{5.26}$$

$$\sum_{i\le k} 2^{-(k+1-i)} V_i V_{n+1}^{k-i} \binom{n+i}{i}_U = \binom{n+k+1}{k}_U, \tag{5.27}$$

and

$$\sum_{i\le k} 2Q^i \Big(\prod_{j=0}^{i-1} V_j\Big)\Big(\prod_{j=0}^{k-1-i} V_{n+k+1-j}\Big)\binom{n+i}{i}_U = \Big(\prod_{i=0}^{k} V_i\Big)\binom{n+k+1}{k}_U, \tag{5.28}$$

where as usual an empty product is equal to 1. The three identities (5.26), (5.27), and (5.28) hold for all integers n and k.

Proof We provide a proof of, say, (5.27). Similar proofs for (5.26) and (5.28) are possible. We perform an induction on k. If $k < 0$, then both sides of (5.27) are zero for all n. Thus, the induction is well based. Fix $\ell \ge -1$, and assume (5.27) holds for $k = \ell$ and all n. We verify that it holds for $k = \ell + 1$ using (5.20):

$$\begin{aligned}
&\binom{n+(\ell+1)+1}{\ell+1}_U \\
&= \frac{V_{\ell+1}}{2}\binom{n+\ell+1}{\ell+1}_U + \frac{V_{n+1}}{2}\binom{n+\ell+1}{\ell}_U \\
&= \frac{V_{\ell+1}}{2}\binom{n+\ell+1}{\ell+1}_U + \frac{V_{n+1}}{2}\sum_{i\le \ell} 2^{-(\ell+1-i)} V_i V_{n+1}^{\ell-i}\binom{n+i}{i}_U \\
&= \frac{V_{\ell+1}}{2}\binom{n+\ell+1}{\ell+1}_U + \sum_{i\le \ell} 2^{-((\ell+1)+1-i)} V_i V_{n+1}^{(\ell+1)-i}\binom{n+i}{i}_U \\
&= \sum_{i\le \ell+1} 2^{-((\ell+1)+1-i)} V_i V_{n+1}^{(\ell+1)-i}\binom{n+i}{i}_U,
\end{aligned}$$

which terminates the inductive proof. □

9. Binomial theorem. The binomial theorem given in the form

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k, \quad (n \ge 0)$$

generalizes into the following Lucasnomial theorem:

$$\prod_{i=0}^{n-1} (x + \alpha^i \beta^{n-1-i}) = \sum_{k=0}^{n} Q^{\binom{n-k}{2}} \binom{n}{k}_U x^k, \quad (n \ge 0) \tag{5.29}$$

where $U(P, Q)$ is a nondegenerate fundamental Lucas sequence and α and β are the zeros of $x^2 - Px + Q$.

Proof We proceed by induction on n. Identity (5.29) holds for $n = 0$ and $n = 1$. Assume it holds for some $n \geq 0$. If we multiply (5.29) through by β^n, distributing one β for each factor on the LHS, and put $y = \beta x$, we obtain writing x instead of y

$$\prod_{i=0}^{n-1}(x + \alpha^i \beta^{n-i}) = \sum_{k=0}^{n} \beta^{n-k} Q^{\binom{n-k}{2}} \binom{n}{k}_U x^k.$$

Multiplying both sides of the above equation by $(x + \alpha^n)$, the LHS is the desired product $\prod_{i=0}^{n}(x+\alpha^i\beta^{n-i})$, while on the RHS, the coefficient c_k of x^k is

$$\begin{aligned} c_k &= \alpha^n \beta^{n-k} Q^{\binom{n-k}{2}} \binom{n}{k}_U + \beta^{n+1-k} Q^{\binom{n+1-k}{2}} \binom{n}{k-1}_U \\ &= \alpha^k \cdot Q^{n-k} Q^{\binom{n-k}{2}} \binom{n}{k}_U + \beta^{n+1-k} Q^{\binom{n+1-k}{2}} \binom{n}{k-1}_U \\ &= Q^{\binom{n+1-k}{2}} \left(\alpha^k \binom{n}{k}_U + \beta^{n+1-k} \binom{n}{k-1}_U \right) \\ &= Q^{\binom{n+1-k}{2}} \binom{n+1}{k}_U, \end{aligned}$$

where the last line comes from (5.7). This completes the induction. □

A formula equivalent to (5.29) but for q-binomial coefficients is proved in [42, Thm. 348] with techniques that date back to Euler. In fact, Ward [80] mentions the 1748 formula of Euler

$$(x + y)(x + qy) \cdots (x + q^{n-1}y) = \sum_{r=0}^{n} \binom{n}{r}_q q^{r(r-1)/2} x^{n-r} y^r.$$

Jarden and Motzkin [44, 45] proved that the product of $n-1$ ($n \geq 1$) second-order recurring sequences, all with characteristic polynomial $x^2 - Px + Q$, is an nth-order linear recurring sequence annihilated by the polynomial

$$f(x) := \sum_{k=0}^{n} (-1)^k \binom{n}{k}_U Q^{k(k-1)/2} x^{n-k}.$$

If α and β are the zeros of $x^2 - Px + Q$, then a product of the form $\prod_{k=1}^{n-1}(c_{1,k}\alpha^t + c_{2,k}\beta^t)$ is clearly annihilated by the polynomial

$$\prod_{i=0}^{n-1}(x - \alpha^i \beta^{n-1-i}).$$

The above polynomial and $f(x)$ have the same degree, and, in fact, we have the identity

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k}_U Q^{k(k-1)/2}x^{n-k}=\prod_{i=0}^{n-1}(x-\alpha^i\beta^{n-1-i}),$$

which is equivalent to (5.29). (Compute $(-1)^n f(-x)$ and change $n-k$ into k to find (5.29).) Also, the formula of Jarden, namely,

$$\prod_{i=0}^{n-1}(x-\alpha^i\beta^{n-1-i})=\sum_{k=0}^{n}(-1)^{\binom{k+1}{2}}\binom{n}{k}_F x^{n-k},$$

appears in Carlitz's work [22], but for the Fibonacci sequence, $F=U(1,-1)$. That is, α and β are the zeros of x^2-x-1.

10. Vandermonde convolution. The Lucasnomial identity

$$\binom{m+n}{k}_U=\sum_i \alpha^{m(k-i)}\beta^{in}Q^{-i(k-i)}\binom{m}{i}_U\binom{n}{k-i}_U, \tag{5.30}$$

where α and β are the zeros of x^2-Px+Q and $U=U(P,Q)$, generalizes the classical Vandermonde convolution

$$\binom{m+n}{k}=\sum_i\binom{m}{i}\binom{n}{k-i}.$$

Identity (5.30) holds for all integers m, n, and k. We begin with proving (5.30) for m and n nonnegative integers and any integer k.

Proof We carry out an induction on $m+n\geq 0$. If $m+n=0$, then $m=n=0$. Both sides are 0 unless $k=0$, in which case both sides are 1. Let us assume (5.30) holds for some $m+n\geq 0$ and all k. Then

$$\begin{aligned}
\binom{m+(n+1)}{k}_U &= \beta^k\binom{m+n}{k}_U+\alpha^{m+n+1-k}\binom{m+n}{k-1}_U\\
&=\beta^k\sum_i\alpha^{m(k-i)}\beta^{in}Q^{-i(k-i)}\binom{m}{i}_U\binom{n}{k-i}_U+\\
&\alpha^{m+n+1-k}\sum_i\alpha^{m(k-1-i)}\beta^{in}Q^{-i(k-1-i)}\binom{m}{i}_U\binom{n}{k-1-i}_U\\
&=\sum_i\alpha^{m(k-i)}\beta^{i(n+1)}Q^{-i(k-i)}\binom{m}{i}_U\times\\
&\left(\beta^{k-i}\binom{n}{k-i}_U+\alpha^{n+1-k+i}\binom{n}{k-1-i}_U\right)\\
&=\sum_i\alpha^{m(k-i)}\beta^{i(n+1)}Q^{-i(k-i)}\binom{m}{i}_U\binom{n+1}{k-i}_U,
\end{aligned}$$

where the first and last equalities come from Equation (5.21). □

To prove (5.30) holds for all m, n, and k, it is convenient to use the equivalent q-Vandermonde convolution identity

$$\binom{m+n}{k}_q = \sum_i q^{(m-i)(k-i)} \binom{m}{i}_q \binom{n}{k-i}_q, \tag{5.31}$$

which can be seen to be equivalent to (5.30) using Equations (5.3) and (5.5). Note that for $q = \alpha/\beta = 1$, we fall back on the usual Vandermonde convolution. If $k < 0$, then both sides of (5.30) are zero. Thus, we assume $k \geq 0$. Say we fix $q > 1$ real, $n \geq 0$ and $k \geq 0$ two integers, then we can view (5.31) as an identity between two real polynomials in $X = q^m$ each of degree k. (For each $0 \leq i \leq k$, $\binom{m}{i}_q$ is a degree-i polynomial in X, while $q^{(m-i)(k-i)} = q^{-i(k-i)} X^{k-i}$ has degree $k-i$.) As (5.31) holds for more than k values of X, i.e., for all q^m, $m \geq 0$, the two sides as polynomials in X must be equal. The coefficients of X^ℓ, $0 \leq \ell \leq k$, are polynomials in $Y := q^n$ of degree at most k on both sides of (5.31). As they agree for all values of $Y = q^n$, $n \geq 0$, more than k values, these polynomials must be identical. Therefore, (5.31) holds for all X and Y, in particular, all $X = q^m$ and $Y = q^n$, m and n in $\mathbb{Z}$.

5.4 Combinatorial Interpretations

If $n \geq k \geq 0$ are two integers, then the binomial coefficient $\binom{n}{k}$ is the number of subsets of size k of a set with n elements. This well-known and useful combinatorial interpretation of binomial coefficients is often taken as a definition. In an xy-coordinate system, $\binom{n}{k}$ is also the number of paths from $(0,0)$ to $(k, n-k)$, or to $(n-k, k)$, where a path is a continuous succession of eastward or northward one-unit steps. Reasons for seeking a simple combinatorial interpretation for Lucasnomials are of at least two kinds. On the one hand, there is an obvious mental satisfaction associated with such a finding. On the other, they are potentially useful: Some identities—identities have two sides—are given new proofs based on counting objects in two different ways, one for each side of the identity. This approach may also suggest new identities. We note that this combinatorial manner of proving identities was the object of a whole book [16].

Existing interpretations of Lucasnomials count weighted tiled paths. But we distinguish two main families of interpretations. Thus, we divide Sect. 5.4 into two subsections.

5.4.1 Square-and-Domino-Tiling Interpretations

Given a rectangular $1 \times n$ board, it is fairly well known that the number of ways to tile this board using square tiles which occupy one cell and dominos which cover two consecutive cells of the board is F_{n+1}, where F_n is the n-th Fibonacci number. A variant of this is: In how many ways can one reach the top of a staircase of n steps if you can go up either one or two steps at once? (In fact, as mentioned earlier, the Fibonacci numbers were known in ancient India well before the days of Leonardo de Pisa: Both in some Sanskrit poetry and Tabla music, the rule was to use short and long syllables or short and long beats twice as long as the short ones. The number of combinations of a given length, thus, was a "Fibonacci" number. In Fibonacci's population dynamics of a group of rabbits, you also have the mature rabbits that reproduce every period and the young ones that become adults after one period and, thus, require two periods to reproduce.) But let us return to our tilings with an example: If $n = 3$, then there are $F_4 = 3$ tilings, namely, sss, ds, and sd, where s and d stand for a square and a domino, respectively. For each "s-and-d" tiling T of an $1 \times n$ board, we define the *weight* $w(T)$ *of the tiling* T as the product of the weights of each of its tiles, i.e., $w(T) = P^s(-Q)^d$. The *weight* $|\mathcal{T}|$ *of a set of tilings* $\mathcal{T}$ is defined as the sum $\sum_{T\in\mathcal{T}} w(T)$. Thus, if $\mathcal{T}_n$ is the set of tilings of a rectangular $1 \times n$ board using squares and dominos, then we find that

$$U_{n+1} = |\mathcal{T}_n|, \tag{5.32}$$

where $U = U(P, Q)$ and, by convention, $|\mathcal{T}_0| = 1$. This follows by induction since tilings in $\mathcal{T}_n$ ending with a square contribute $P|\mathcal{T}_{n-1}|$ to $|\mathcal{T}_n|$ and tilings ending with a domino contribute $(-Q)|\mathcal{T}_{n-2}|$. Hence, $|\mathcal{T}_n| = P|\mathcal{T}_{n-1}| - Q|\mathcal{T}_{n-2}|$. Clearly, $|\mathcal{T}_1| = P = U_2$ and $|\mathcal{T}_2| = P^2 - Q = U_3$. Note that if $P \geq 1$ and $-Q \geq 1$, then tiling weights bear a concrete interpretation: We may think of squares coming in P different colors and dominos in yet $-Q$ distinct other colors. The Fibonacci case is singular as $P = -Q = 1$ so that the weight $|\mathcal{T}|$ of a set of tilings $\mathcal{T}$ is simply the cardinality of $\mathcal{T}$. Note that our use of squares and dominos as the tiling modus operandi is linked to our observation (2.30) that $U_n(P, Q) = \Psi_n(P, Q)$, where Ψ_n is a homogeneous polynomial of degree $n - 1$, if the variable P has degree 1 (the length of a square tile) and Q has degree 2 (the length of a domino).

Example 79 The number of tilings with squares and dominos of a $1\times(m-1)$ rectangular board is F_m. Consider the number of such tilings that use a domino d to cover the two consecutive cells n and $n + 1$. There are F_n ways of tiling the initial cells $1, \ldots, n-1$, and F_{m-n-1} ways of tiling the $m-n-2$ final cells $n+2, \ldots, m-1$. Hence, there are F_nF_{m-n-1} ways of simultaneously tiling the cells left of d and the cells right of d. The remaining tilings do not have a domino straddling over cells n and $n+1$. So we can tile the first n cells (in F_{n+1} ways) and the last $m - n - 1$ cells (in F_{m-n} ways) independently. Therefore, $F_m = F_nF_{m-n-1}+F_{n+1}F_{m-n}$. With P-weighted squares and $-Q$-

weighted dominos, the same argument carries over, but the domino d has weight $-Q$, so this reasoning yields a combinatorial proof of the important identity (2.42), i.e., $U_m = U_{n+1}U_{m-n} - QU_nU_{m-n-1}$. □

Thus, the numerator $U_nU_{n-1}\cdots U_{n-k+1}$ of $\binom{n}{k}_U$ can be interpreted as the number of simultaneous square and domino (weighted) tilings of a collection of boards of respective length $n-1, n-2, \ldots, n-k$. Using this interpretation, Benjamin and Plott [17] were able to describe a procedure by which one could view the denominator $U_k \cdots U_1$ of $\binom{n}{k}_U$ as subtilings of the numerator. Their procedure provided a first combinatorial explanation of the integrality of Lucasnomials.

Interestingly, the associated Lucas sequence number $V_n = V_n(P, Q)$, $n \geq 1$, counts the number of *circular* weighted tilings of a $1 \times n$ rectangular board. The tilings are made of squares and dominos with the same respective weights of P and $-Q$, but it is possible to have a domino straddling over the n-th and the 1-st cells. These are sometimes called *bracelet* tilings. Thus, if $n = 2$, then we can tile in three ways, two squares, or in two ways, one domino, giving $V_2 = P^2 - 2Q$.

Example 80 We may prove again the first identity in (2.26), i.e., $V_m = U_{m+1} - QU_{m-1}$, by observing that there are two kinds of tilings of a length-m bracelet: the $-QU_{m-1}$ tilings with one domino covering both cells m and 1 and the U_{m+1} tilings with no such domino. □

In 2010, two combinatorial interpretations of Lucasnomials $\binom{m+n}{m}_U$ were found by Sagan and Savage [71]. The second uses circular tilings. We only describe the first. Any lattice path from $(0, 0)$ to (m, n), where m and n are positive integers, i.e., a path consisting of $m+n$ unit steps, m going eastward and n northward, leaves n rows $(m_1, m_2, \ldots, m_n)$ on its left, bounded by the y-axis, and m columns $(n_1, n_2, \ldots, n_m)$ below the path and bounded southward by the x-axis. By tiling each row m_i, $1 \leq i \leq n$, and each column n_j, $1 \leq j \leq m$, with squares and dominos with the caveat that the tilings of the columns—to be legal—have to begin with a domino, we associate a weight to the given path. Here, the weight of one particular tiling of the m rows and n columns is the product of the individual weights of each row and column. The *path weight* is the sum of the weights of all legal tilings of the set of rows and columns associated with the path. Then $\binom{m+n}{m}_U$ is the sum of the path weights over all paths from $(0, 0)$ to (m, n). If a column has 0 height, i.e., if $n_j = 0$, then this column is tiled with the empty tiling, which has a weight of 1. Although it does not begin with a domino, it is still legal. If the j-th column has only one cell, i.e., if $n_j = 1$, then no legal tiling exists, and the path weight is zero. Such a path does not contribute to $\binom{m+n}{m}_U$. If $U = F$, then all legal tilings have weight 1. Thus, $\binom{m+n}{m}_F$ counts the number of ways of drawing a path from $(0, 0)$ to (m, n) and legally tiling the rows and columns. Hence, for a simple example, we choose $U = F$, $m = 3$, and $n = 2$. Of the ten paths from $(0, 0)$ to $(3, 2)$, only four contribute, namely,

$p_1 = NNEEE$, $p_2 = ENNEE$, $p_3 = EENNE$, and $p_4 = EEENN$. The two northward steps have to cling together for the path to have a legal tiling. The paths p_1 and p_2 have a weight of 1 because there is only one way to tile each of its rows and columns. Path p_3 has weight $2 \times 2 \times 1 \times 1 \times 1 = 4$ for its two rows each have two tilings, while p_4 has weight $3 \times 3 = 9$ from its two rows of length three. Thus, the sum of the weights of all the legal paths is

$$1 + 1 + 4 + 9 = 15 = (5 \cdot 3)/(1 \cdot 1) = (F_5 \cdot F_4)/(F_2 \cdot F_1) = \binom{5}{2}_F.$$

Remark 28 If instead of the Fibonacci sequence $F = U(1, -1)$, we chose $I = U(2, 1)$, the identity sequence, then squares have weight 2 and dominos weight -1. Thus, using the above example,

$$\begin{aligned}\sum_{i=1}^{4} w(p_i) &= (-1)^3 + 2^2(-1)^2 + (2^2 + (-1))^2(-1) + (2^3 + (-1)2 + 2(-1))^2 \\ &= -1 + 4 - 9 + 16 = 10,\end{aligned}$$

which is the binomial coefficient $\binom{5}{2}$ as expected. However, this is certainly a roundabout way of counting the number of paths from $(0, 0)$ to $(3, 2)$. This remark points out a drawback of the interpretation in which, ideally, we would like to count paths in a natural way when dealing with ordinary binomial coefficients.

A few years later [18], these two interpretations of Lucasnomials were restated in simple terms and illustrated with examples, mostly in the Fibonacci case. A couple of identities were combinatorially explained, and a few simple and appealing Fibonomial identities, taken from the existing literature, were listed as awaiting interpretation.

Writing $k!_F$ for $F_k F_{k-1} \cdots F_1$, $(k \geq 1)$, the combinatorial interpretation given by Sagan and Savage implies that

$$(m + n)!_F = m!_F \cdot n!_F \cdot \sum_p \ell_p, \tag{5.33}$$

where p is a path from $(0, 0)$ to (m, n) and ℓ_p is the number of legal tilings of the n rows and m columns associated with p. Viewing $k!_F$ as the number of ways of simultaneously tiling (with squares and dominos) k rows of respective lengths $k - 1, k - 2, \ldots, 0$, Killpatrick and Weaver [46] produced an explicit combinatorial bijection, as we may say, between the two sides of Equation (5.33).

Recently [19], another combinatorial interpretation was discovered. It is similar, and in some sense isomorphic, to the Sagan and Savage interpretation we just described (see [19, end of Sect. 2]), yet more natural and apparently

more fruitful. In particular, it led to a first interpretation of Lucasnomial Catalan numbers, which we describe in Sect. 5.5.3.

Let s_n be the upward staircase path which starts at the point $(n, 0)$ and ends at $(0, n)$ alternating west and northward unit steps:

$$(n, 0) \to (n-1, 0) \to (n-1, 1) \to (n-2, 1) \to \cdots \to (0, n-1) \to (0, n).$$

The staircase-shape region $\mathcal{S}_n$ to the right of the y-axis, below the path s_n and above the x-axis, consists of $n-1$ horizontal rows of square boxes. Going upward, these rows are of respective lengths $n-1, n-2, \ldots, 1$. A tiling of $\mathcal{S}_n$ is a tiling of each of these $n-1$ rows with squares and dominos. If, as before, a square tile has weight P and a domino has weight $-Q$, then there are $U_n U_{n-1} \cdots U_1$ distinct tilings of $\mathcal{S}_n$. Here, $U = U(P, Q)$.

Let k, $0 \le k \le n$, be a fixed integer throughout the interpretation, since this interpretation is specific to the Lucasnomial $\binom{n}{k}_U$. We begin by describing how, to any given tiling T of $\mathcal{S}_n$, we associate a unique path p through $\mathcal{S}_n$. The path p begins at the point $(k, 0)$ and ends at $(0, n)$ and is constructed uniquely as follows:

The path is made of a succession of unit steps going either north or west. The path p moves northward unless we step out of the region $\mathcal{S}_n$, or unless a northward edge would cross over through the center of a domino in T, and, in these two cases, the path moves west. Note that a westward step is necessarily followed by a northward step, because of the staircase shape of $\mathcal{S}_n$ and because dominos have length 2.

Two tilings T_1 and T_2 of $\mathcal{S}_n$ are *equivalent* if their associated paths p coincide. The number of tilings of an equivalence class will be shown to be a multiple of $D_k = (U_k \cdots U_1)(U_{n-k} \cdots U_1)$. Therefore, $U_n U_{n-1} \cdots U_1$, the number of tilings of $\mathcal{S}_n$, i.e., of all rows in $\mathcal{S}_n$, must be a multiple of D_k, and $\binom{n}{k}_U$ be an integer.

But let us return to the path p associated with T. A northward step immediately following a westward step is called an NL step, because the two successive steps draw an L. Other northward steps are called NI steps. Construct a partial tiling $B = B_T$, a subtiling of T, by, in a given row, erasing the tiles that lie left of an NL step and erasing the tiles that lie to the right of NI steps. Note that two tilings of $\mathcal{S}_n$ which produce the same partial tiling B must lie in the same equivalence class. The number of ways of completing the partial tiling B into a full tiling of $\mathcal{S}_n$ is D_k. Indeed, p must have k NL steps, and the i-th NL step has $k-i$ blank cells on its left, for $1 \le i \le k$. Thus, $k-i$ varies from $k-1$ to 0, and these blank partial rows can be tiled in $U_k \cdots U_1$ ways. There must be $n-k$ NI steps for the path p to reach the final point $(0, n)$ at altitude n. The i-th NI step, $1 \le i \le n-k$, must have $n-k-i$ blank cells on its right, because, due to the staircase shape of $\mathcal{S}_n$, the number of cells right of an NI step is not affected by the number of NL steps that precede it. Thus, the blank partial rows right of NI steps can be tiled in $U_{n-k} \cdots U_1$ ways. Therefore, $w(T) = D_k \cdot w(B)$. An example of a tiling T

in $\mathcal{S}_6$ is illustrated in Fig. 5.1, where an NI step is designated by an N and a west step followed by a north step by WN.

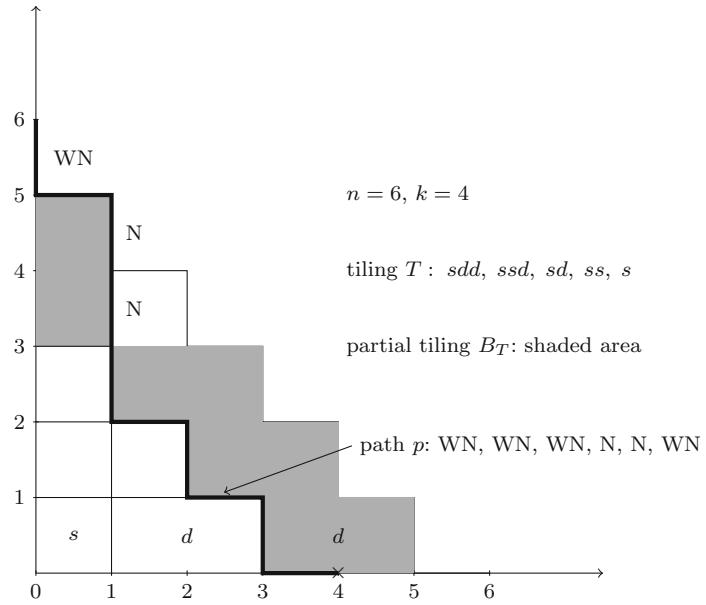


Fig. 5.1 Example in $\mathcal{S}_6$

We will say that a path p in $\mathcal{S}_n$ from $(k,0)$ to $(0,n)$ is *tilable* if it is associated with a tiling T of $\mathcal{S}_n$ in the way previously described. Note that not all $\binom{n}{k}$ lattice paths from $(k,0)$ to $(0,n)$ made of westward and northward steps with no two consecutive westward steps are tilable. For instance, only three of the six such paths through $\mathcal{S}_4$ starting at $(2,0)$ are tilable. A partial tiling B is said to *belong to* p, and we write $B \in p$, if $B = B_T$ for some tiling T of $\mathcal{S}_n$ with which p is associated. Two equivalent tilings do not usually produce the same partial tiling, because the non-erased parts of these tilings do not usually agree. If B is the partial tiling derived from T, we showed above that $w(T) = D_k \cdot w(B)$. Therefore,

$$U_n \cdots U_1 = |\mathcal{S}_n| = \sum_p |Cl(p)| = \sum_p \sum_{B \in p} w(B) \cdot D_k, \tag{5.34}$$

where the sums are over all tilable paths p from $(k,0)$ to $(0,n)$ and $Cl(p)$ is the class of all tilings to which the same path p is associated with. Thus, the Lucasnomial $\binom{n}{k}_U$ is interpreted as a sum of weights of partial tilings. That is,

$$\binom{n}{k}_U = \sum_p \sum_{B \in p} w(B), \tag{5.35}$$

where the outer sum is over all tilable paths p from $(k,0)$ to $(0,n)$.

5.4.2 An Interpretation Coming from q-Binomial Coefficients

We begin with a well-known interpretation of q-binomial coefficients and mention two of its isomorphic variants before seeing how this interpretation carries over to Lucasnomials.

Indeed, the Gaussian coefficient $\binom{n}{k}_q$ is well known to count weighted paths from $(0,0)$ to $(k, n-k)$. These paths are non-decreasing in that they use only northward or eastward unit steps. To be precise, the identity

$$\binom{n}{k}_q = \sum_{a=0}^{k(n-k)} c_a q^a \tag{5.36}$$

holds, where c_a is the number of paths from $(0,0)$ to $(k, n-k)$ such that the area under the path and above the x-axis is a. Thus, the weight of a path of area a is q^a. When $q = 1$, all paths have weight 1 and $\binom{n}{k}_q = \binom{n}{k}$, which simply counts paths. As observed in Remark 28, interpretations of Lucasnomials given in [19, 71] have the drawback of not falling back on this natural interpretation of ordinary binomial coefficients.

Konvalina [51, eq. (19)] observed that the q-binomial coefficient $\binom{n}{k}_q$ satisfies the identity

$$\binom{n}{k}_q = \sum_{0 \le i_1 \le i_2 \le \cdots \le i_k \le n-k} q^{i_1+i_2+\cdots+i_k}, \tag{5.37}$$

which he interpreted by using boxes and balls. Suppose there are $n-k+1$ boxes, where box i, $0 \le i \le n-k$, contains q^i balls. Then $\binom{n}{k}_q$ is the number of ways of selecting k boxes and one ball from each box. The same box may be chosen several times, the ball being returned to its box, if formerly chosen. Note that this interpretation is in one-to-one correspondence with the above area-weighted path interpretation. Say we walk along a given path from $(0,0)$ to $(k, n-k)$. We will encounter exactly k horizontal edges of successive heights $0 \le h_1 \le h_2 \le \cdots \le h_k \le n-k$. The vector $(h_1, h_2, \ldots, h_k)$ actually defines the path and corresponds to choosing the boxes numbered $h_1, h_2, \ldots, h_k$. The number of ways of choosing the k balls is $q^{\sum_j h_j}$, which is q^a, where a is the area subtended by our path.

Recently, a variant of the above interpretation of q-binomial coefficients was exploited to explain combinatorially various q-identities [3]. The authors chose to work with a tiling interpretation "isomorphic" to the weighted path counting (5.36). That is, there is a one-to-one weight-preserving correspondence between paths and tilings. Tile a $1 \times n$ board with n square tiles, k blue and $n-k$ of color red. Walking along the path from $(0,0)$ to $(k, n-k)$, place a red tile for a north step and a blue one for an eastward step. The

weight of a red tile is 1, and the weight of a blue one is q^i, if that blue tile is preceded by i red tiles. The weight of the board tiling is the product of the weights of individual tiles. This bijection clearly preserves weight as the area below an eastward step matches the number of northward steps that precede it. Thus, $\binom{n}{k}_q$ is the number of tilings of a $1 \times n$ board with exactly k blue tiles.

The identity

$$\binom{n}{k}_q = \binom{n-1}{k}_q + q^{n-k}\binom{n-1}{k-1}_q, \tag{5.38}$$

for instance, is easily seen to hold using this interpretation. Indeed, tilings that end with a blue tile contribute $q^{n-k}\binom{n-1}{k-1}_q$, while tilings that end with a red tile contribute $\binom{n-1}{k}_q$. The symmetry identity $\binom{n}{k}_q = \binom{n}{n-k}_q$ is explained within the frame of this tiling interpretation in [3, p. 101]. Identity (5.6) may then be obtained by reasoning as we did for identity (5.38). Consider the set of tilings of a $1 \times n$ board with $n-k$ blue tiles. The contribution of tilings that end with a blue tile is $q^k\binom{n-1}{n-k-1}_q = q^k\binom{n-1}{k}_q$, while the contribution of those ending with a red tile is $\binom{n-1}{n-k}_q = \binom{n-1}{k-1}_q$.

Finally, we observe that the area-weighted path, and correspondingly the box-and-ball choosing or the weighted tiling interpretations of q-binomial coefficients, generalizes to Lucasnomials. Suppose Lucasnomials satisfy a Pascal-like relationship

$$\binom{n}{k}_U = x_k\binom{n-1}{k}_U + y_{n-k}\binom{n-1}{k-1}_U, \tag{5.39}$$

for all integers n and k, for some sequences (x_n) and (y_n). (Note that taking $n = 1$ and $k = 0$ implies $x_0 = 1$, while $n = k = 1$ yields $y_0 = 1$.) Say a horizontal (eastward) edge of height h has weight y_h and a vertical (northward) edge at distance d from the y-axis, i.e., of abscissa d, has weight x_d. Define the weight of a path from $(0,0)$ to $(k, n-k)$ as the product of the weights of its edges. Then $\binom{n}{k}_U$ is the sum of the weights of all paths from $(0,0)$ to $(k, n-k)$. This can be seen by induction on n using (5.39). Note that $\binom{1}{0}_U = 1$ and the only path from $(0,0)$ to $(0,1)$ is made of a vertical edge of abscissa 0 and, thus, of weight $x_0 = 1$. Similarly, $\binom{1}{1}_U = 1$, and the one-edge path from $(0,0)$ to $(1,0)$ has weight $y_0 = 1$. Paths from $(0,0)$ to $(k, n-k)$ that reach $(k, n-k)$ through $(k-1, n-k)$ followed by a horizontal edge of height $n-k$ account for a cumulative weight equal to $y_{n-k}\binom{n-1}{k-1}_U$. The other paths must go through $(k, n-k-1)$ and end with a vertical edge of abscissa k. Hence, their cumulative weight is $x_k\binom{n-1}{k}_U$. The conclusion follows from (5.39).

The corresponding "isomorphic" tiling interpretation of $\binom{n}{k}_U$ uses a $1 \times n$ board with k blue and $n-k$ red square tiles. The weight of a blue tile, which is preceded by m red tiles, is y_m, and the weight of a red tile, preceded by

m blue tiles, is x_m. The weight of a tiling is the product of all the individual weights of its tiles. Then $\binom{n}{k}_U$ is the sum of the weights of all tilings that use k blue tiles and $n-k$ red ones (or vice versa).

Note that the Pascal-like identities (5.6), (5.7), (5.13), (5.20), and (5.21) are all special cases of the general type (5.39).

Let us put to use this tiling interpretation mimicking an argument made in [3] in the context of Gaussian coefficients. The argument works if we require the sequences (x_n) and (y_n) to be geometric.

Theorem 81 *Suppose U is a fundamental Lucas sequence and (x_m) and (y_m) are geometric sequences for which (5.39) holds. Then*

$$\binom{2n}{n}_U = \sum_{k=0}^{n} x_k^k \, y_{n-k}^{n-k} \binom{n}{k}_U^2. \tag{5.40}$$

Proof A tiling of a $1 \times 2n$ board with n red and n blue tiles can always be viewed as a concatenation, $(1 \times n) \times (1 \times n)$, of two consecutive half-boards. If there are k blue tiles in the first half-board, then there are $n-k$ in the second half-board. Each of the k red tiles in the second half-board sees its local weight (i.e., its weight within this second half-board) multiplied by x_k due to the presence of the extra k blue tiles in the first half-board. Each of the $n-k$ blue tiles in that second half has an extra $n-k$ red tiles to its left lying in the first half-board. It sees its weight multiplied by y_{n-k}. Globally, we have to multiply the product of the weights of the two half-boards $\binom{n}{k}_U \times \binom{n}{n-k}_U$ by the factor $x_k^k \cdot y_{n-k}^{n-k}$. Summing over all possible k yields the result. □

The identities (5.7) and (5.21) involve geometric sequences. Thus, using, say, (5.7), we obtain

$$\binom{2n}{n}_U = \sum_{k=0}^{n} \alpha^{k^2} \beta^{(n-k)^2} \binom{n}{k}_U^2. \tag{5.41}$$

It is easy to verify that if (5.39) holds with (x_m) and (y_m) geometric, i.e., with $x_m = a^m$ and $y_m = b^m$ for all $m \geq 0$, then $a + b = P$ and $ab = Q$. Hence, (5.39) is necessarily one of the two identities (5.7) or (5.21).

5.5 Lucasnomial Catalan Numbers

5.5.1 Introduction

The Catalan numbers C_n, although they pop up in various areas of mathematics and have very many combinatorial interpretations, are often defined via the simple algebraic expression

$$C_n = \frac{1}{n+1}\binom{2n}{n}. \tag{5.42}$$

It is not necessarily immediate from (5.42) that they are integers. However, C_n is the difference $\binom{2n}{n} - \binom{2n}{n-1}$. We have $C_0 = C_1 = 1$, $C_2 = 2$, $C_3 = 5$, $C_4 = 14$, $C_5 = 42$, $C_6 = 132$, and $C_7 = 429$. The ratio C_{n+1}/C_n tends to 4 as n tends to infinity. They satisfy the convolution identity $C_{n+1} = \sum_{i=0}^{n} C_i C_{n-i}$. Their generating function C satisfies $xC^2 - C + 1 = 0$ and is $\frac{1-\sqrt{1-4x}}{2x}$. A rich book [76] was written on their various combinatorial interpretations, properties, and generalizations. Here, we single out two specific generalizations, the *Fuss-Catalan* and the *generalized Fuss-Catalan* numbers. Given $a \geq 2$ and $r \geq 1$ integers, the generalized Fuss-Catalan numbers $C_{a,r}(n)$ are defined as

$$C_{a,r}(n) = \frac{r}{(a-1)n+r}\binom{an+r-1}{n} = \frac{r}{an+r}\binom{an+r}{n}, \tag{5.43}$$

for all $n \geq 0$, and are integers. In fact, they possess at least one combinatorial interpretation, counting Raney sequences [33, pp. 359–363]. The Fuss-Catalan numbers correspond to the case $a \geq 2$ and $r = 1$ and have many interpretations that extend some interpretations of the Catalan numbers.

We next illustrate how a few classical interpretations of the Catalan numbers extend to $C_{3,1}(n)$. The Catalan number C_n is:

1. The number of triangulations of a convex $(n+2)$-gon into n triangles (using $n-1$ non-intersecting diagonals)
2. The number of meaningful parenthesizations in the product of $n+1$ elements $a_1 * a_2 * \cdots * a_{n+1}$, where $*$ is a binary operation
3. The number of paths with $(1,0)$ or $(0,1)$ moves from $(0,0)$ to (n,n) which start with a $(1,0)$ move and do not cross over the line $y = x$
4. The number of ballot sequences of length $2n$, i.e., finite sequences $(a_i)_{1 \leq i \leq 2n}$ with terms $a_i = \pm 1$, nonnegative partial sums $\sum_{i=1}^{k} a_i$, and zero complete sum $\sum_{i=1}^{2n} a_i = 0$
5. The number of non-crossing partitions of $[n] = \{1, 2, \ldots, n\}$, i.e., such that if $a < b < c < d$, a and c belong to the same block B, b and d to B', then $B = B'$
6. The number of binary trees with n vertices

Correspondingly, we find that $C_{3,1}(n) = \frac{1}{2n+1}\binom{3n}{n}$, the n-th Fuss-Catalan number with $a = 3$, is:

1. The number of slicings of a $(2n+2)$-polygon into n quadrilaterals
2. The number of meaningful parenthesizations in the product of $2n+1$ elements $a_1 * a_2 * \cdots * a_{2n+1}$, where $*$ is a ternary operation (elements are multiplied three at a time)

3. The number of paths with $(1,0)$ or $(0,1)$ moves from $(0,0)$ to $(2n,n)$ which start with a $(1,0)$ move and do not cross the line $x = 2y$
4. The number of finite sequences of length $3n$, $(a_i)_{1\le i\le 3n}$, with terms $a_i \in \{1,-2\}$ and nonnegative partial sums $\sum_{i=1}^{k} a_i$ and $\sum_{i=1}^{3n} a_i = 0$
5. The number of non-crossing partitions of $[2n]$ into blocks all of even cardinality
6. The number of planar ternary trees with $2n+1$ vertices

The point of this section is to present some generalizations of Catalan numbers with respect to Lucas sequences and some recent work on these generalizations. Clearly, there is much yet to discover.

5.5.2 Definition and Integrality

Given a nondegenerate fundamental Lucas sequence $U = U(P,Q)$ and integers $a \ge 2$ and $r \ge 1$, it is easy and tempting to define *generalized Lucasnomial Fuss-Catalan* numbers $C_{U,a,r}(n)$ as

$$C_{U,a,r}(n) = \frac{U_r}{U_{(a-1)n+r}} \binom{an+r-1}{n}_U = \frac{U_r}{U_{an+r}} \binom{an+r}{n}_U, \tag{5.44}$$

in algebraic analogy to (5.43). If $r = 1$, then we obtain the *Lucasnomial Fuss-Catalan* numbers

$$C_{U,a}(n) = C_{U,a,1}(n) = \frac{1}{U_{(a-1)n+1}} \binom{an}{n}_U. \tag{5.45}$$

The *Lucasnomial Catalan* numbers $C_U(n) := C_{U,2,1}(n)$ are defined by

$$C_U(n) = \frac{1}{U_{n+1}} \binom{2n}{n}_U. \tag{5.46}$$

When U is the Fibonacci sequence F, then they are known as *Fibonomial Catalan* numbers. Here as in other instances in the theory of Lucas sequences, the discovery of these Lucasnomial Catalan generalizations came from two independent sources: the Fibonacci and the q-numbers. On the Fibonacci side, the discovery seems to date to the early 1970s when Gould [36] listed the first 50 Fibonomial Catalan numbers. Gould [35] gave a proof of their integrality. This proof would in fact carry over to all Lucasnomial Catalan numbers for U a regular sequence. Actually, replacing n and k by, respectively, $2n$ and n in Equation (5.13), one obtains

$$\binom{2n}{n}_U = U_{n+1} \binom{2n-1}{n}_U - QU_{n-1} \binom{2n-1}{n-1}_U,$$

which, after division by U_{n+1}, is readily seen to yield

$$C_U(n) = \binom{2n-1}{n}_U - Q\binom{2n-1}{n-2}_U, \tag{5.47}$$

as noted in [25]. Thus, Lucasnomial Catalan numbers are integers with no restrictive hypotheses on U. Lucasnomial Fuss-Catalan numbers are also integers for all choices of U; see [13, Thm. 6]. A combinatorial interpretation of Lucasnomial Fuss-Catalan numbers, valid for all choices of U, was found recently [19], as we will see in Sect. 5.5.2. Incidentally, this interpretation provides a second integrality proof. Generalized Lucasnomial Fuss-Catalan numbers were shown to have a nonnegative p-adic valuation for all regular primes p in [13, Thm. 9] and so to be integers for U regular. Their valuation with respect to a special prime p was shown to be nonnegative a little later [15, Thm. 6]. Hence, generalized Lucasnomial Fuss-Catalan numbers are always integers as well. However, to this day, no combinatorial interpretation for these numbers is known.

On the q-number side, several q-generalizations of the Catalan numbers were discovered and studied in the 1960s and 1970s by MacMahon, Carlitz, and Pólya in particular (see [30] for a list of references). They were called q-Catalan numbers. Further encompassing generalizations [30] were proposed and given combinatorial interpretations. One may also consult Exercise A43 [76, p. 121].

The Carlitz q-Catalan numbers $c_q(n)$ derive very naturally from both the interpretation (5.36) of Gaussian coefficients and the interpretation **3.** of the Catalan numbers stated in Sect. 5.5.1. They satisfy

$$c_q(n) = \sum_{p \in \mathcal{C}_n} q^{a(p)}, \tag{5.48}$$

where $\mathcal{C}_n$ is the set of Catalan paths, i.e., paths from $(0,0)$ to (n,n) that remain below the segment joining $(0,0)$ to (n,n). Here, $a(p)$ is the area subtended by the path p. Actually, they were given the equivalent interpretation

$$c_q(n) = \sum_{w \in \mathcal{W}_n} q^{\mathrm{inv}(w)}, \tag{5.49}$$

where $\mathcal{W}_n$ is the set of binary words $w = w_1 w_2 \cdots w_{2n}$ of length $2n$ such that the number of 1s never exceeds the number of 0s in any prefix of the word w and $\mathrm{inv}(w)$ is the number of inversions, i.e., of (i,j)s, $i < j$, such that $w_i > w_j$. Each such word is in bijection with a Catalan path if a 0 corresponds to a horizontal edge and a 1 to a vertical edge. A moment of thought and one sees that the area under a path is also the sum of the row areas east of vertical edges, which is what inversions measure.

Another natural q-generalization of Catalan numbers is obtained from (5.46) on replacing U_n by the q-number $\frac{q^n-1}{q-1}$. This generalization was traced back to MacMahon [57, Vol. 2, p. 214] in the paper [30]. The *MacMahon q-Catalan* numbers $C_q(n)$ had the following combinatorial interpretation:

$$C_q(n) = \sum_{w \in \mathcal{W}_n} q^{\mathrm{maj}(w)}, \tag{5.50}$$

where $\mathcal{W}_n$ is the set of binary words $w = w_1 w_2 \cdots w_{2n}$ as defined above and $\mathrm{maj}(w)$, the major index of w, is the sum $\sum_{\{1 \le i < 2n;\, w_i > w_{i+1}\}} i$. For instance,

$$\begin{aligned} C_q(3) &= \frac{1}{\frac{q^4-1}{q-1}} \cdot \binom{6}{3}_q = \frac{(q^6-1)(q^5-1)}{(q^3-1)(q^2-1)} = \frac{(q^3+1)(q^5-1)}{(q+1)(q-1)} \\ &= (q^2-q+1)(q^4+q^3+q^2+q+1) = q^6+q^4+q^3+q^2+1. \end{aligned}$$

The five sequences in $\mathcal{W}_3$ contribute, respectively,

$$\begin{array}{ll} 000111 & q^0 = 1 \\ 001011 & q^3 \\ 001101 & q^4 \\ 010011 & q^2 \\ 010101 & q^{2+4} = q^6 \end{array}$$

Remark 29 The number $C_q(n)$ is also a sum of weighted paths. Indeed, the interpretation of $C_q(n)$ using the major index has an isomorphic weighted path interpretation when, in place of $\mathcal{W}_n$, we return to the set of Catalan paths $\mathcal{C}_n$. Define the weight of a Catalan path as the product of the weights of all its edges, where a horizontal edge of height h has weight q^h but only if that edge is immediately followed by a vertical edge. Similarly, the weight of a vertical edge of abscissa d is q^d, if it is immediately preceded by a horizontal edge and if $d < n$. All other edges have weight 1. Then

$$C_q(n) = \sum_{p \in \mathcal{C}_n} w(p),$$

where $w(p)$ is the weight of the path p.

Remark 30 The identity (5.47) applied to q-binomial coefficients yields

$$C_q(n) = \binom{2n-1}{n-1}_q - q\binom{2n-1}{n-2}_q.$$

With the tiling interpretation of q-binomial coefficients with red and blue square tiles, isomorphic to the area-weighted interpretation, the above identity gives a combinatorial interpretation of $C_q(n)$ as tiling weights of $1 \times 2n$

boards with $n+1$ blue tiles. It is the weight of all such tilings that start with a blue tile *minus* the weight of all those tilings such that the last blue tile is immediately preceded by a red tile.

It would be worth examining whether the various q-Catalan numbers and their interpretations could find extensions in the context of Lucasnomials.

5.5.3 Interpretation of Lucasnomial Catalan Numbers

The only existing combinatorial interpretation of Lucasnomial Catalan numbers $C_U(n)$ to date [19] is based on a small alteration of the interpretation of Lucasnomials obtained in (5.35) at the end of Sect. 5.4.1. We now describe it with the notation and terminology we had used to obtain (5.35).

Consider the region $\mathcal{S}_{2n}$ and a tiling T of $\mathcal{S}_{2n}$. Assume $k = n-1$. Let p be the path from $(n-1,0)$ to $(0,2n)$ associated with T. Then $B = B_T$ is the partial tiling obtained from T by erasing tiles right of NI steps and left of NL steps. A subtiling C of T, slightly modified from B, is now defined. The *Catalan partial tiling* C is identical to B in all rows except for the initial row of length $2n-1$. The first row of C is left fully untiled if the initial step of p is northward, i.e., if it is an NI step. So compared to B, the tiling C has an additional string of $n-1$ empty cells left of the NI step. If the initial step is westward, yielding an NL step, then C only retains the domino east of that NL step, thus leaving an extra string of $(2n-1)-(n-2)-2 = n-1$ blank cells to the right of the domino compared with B. Note in passing that $C = C_T$ is sufficient to re-trace the path p associated with T. By (5.32), $w(B) = w(C) \times w(1 \times (n-1)$ board$) = w(C) \cdot U_n$. If B is derived from T, then $w(T) = D_{n-1} \cdot w(B)$. Since $|\mathcal{S}_{2n}| = \sum_p \sum_{B \in p} w(B) \cdot D_{n-1}$, we find that

$$\frac{|\mathcal{S}_{2n}|}{U_n D_{n-1}} = \frac{1}{U_n} \binom{2n}{n-1}_U = \sum_p \sum_C w(C).$$

Hence, as the Lucasnomial Catalan number $C_U(n) = \frac{1}{U_{n+1}} \binom{2n}{n}_U$ is equal to $\frac{1}{U_n} \binom{2n}{n-1}_U$, we see that

$$C_U(n) = \sum_p \sum_C w(C), \tag{5.51}$$

where the outer sum is over all tilable paths p from $(n-1,0)$ to $(0,2n)$ and the inner sum over all Catalan partial tilings C associated with p.

Remark 31 The above interpretation is applicable to explaining combinatorially the identity (5.47); see [19, Prop. 4.3].

Extending the idea presented above, i.e., by defining partial tilings from paths in $\mathcal{S}_{(a+1)n}$, the authors [19] also provided a combinatorial interpretation of Lucasnomial Fuss-Catalan numbers

$$C_{U,a}(n) = \frac{1}{U_{an+1}} \begin{pmatrix} (a+1)n \\ n \end{pmatrix}_U.$$

5.5.4 The Search for Catalan-Like Triples

Given a nondegenerate Lucas sequence $U = U(P, Q)$ and integers $a \geq 2$ and k, define $D_{U,a,k}$ as the set of positive integers n such that $U_{(a-1)n+k}$ divides $\binom{an}{n}_U$. The complementary set of $D_{U,a,k}$ in the positive integers is denoted by $\overline{D}_{U,a,k}$. Because for all integers n, $|U_n(P, Q)| = |U_n(-P, Q)|$, the two sets $D_{U(P,Q),a,k}$ and $D_{U(-P,Q),a,k}$ are identical. Hence, we may and will assume that $P > 0$.

If $k = 1$, then since Lucasnomial Fuss-Catalan numbers (5.45) are integers, $D_{U,a,1} = \mathbb{N}$. Are there other triples (U, a, k) with $k \neq 1$ for which $D_{U,a,k} = \mathbb{N}$? Such triples are called *Catalan-like triples* for obvious reason. If $U = U(2, 1) = I$, the sequence of natural numbers, then there are no Catalan-like triples of type (I, a, k) with $k \neq 1$. Pomerance [69, Thm. 1] showed that $\overline{D}_{I,2,k}$ is infinite when $k \neq 1$ with a marked difference in the size of $D_{I,2,k}$ depending on whether $k \leq 0$ or $k \geq 1$. If $k \leq 0$, then $D_{I,2,k}$ has an upper asymptotic density less than 0.25135. If $k \geq 1$, then $D_{I,2,k}$ has asymptotic density 1; see [69, Thm. 2].

A subset S of the positive integers has an asymptotic density equal to $d = d(S) \in [0, 1]$ if a certain limit exists and is d, i.e., if

$$\lim_{N \to \infty} \frac{\#S(N)}{N} = d,$$

where $\#S(N)$ is the number of integers n in S within the interval $[1, N]$. The upper asymptotic density of S, $\bar{\delta}(S)$, is the upper limit, or the limsup (or $\overline{\lim}$), of the sequence $(\#S(n)/n)$. The lower asymptotic density of S is given by the liminf of $(\#S(n)/n)$.

Pomerance [69, Thm. 3] had shown that if $k \leq 0$, then $D_{I,2,k}$ is infinite, but small with $\bar{\delta}(D_{I,2,k}) \leq 1 - \log 2$, a bound that was lowered to $1 - \log 2 - 0.05551 \approx 0.25134$ by Sanna [72]. The argument of Pomerance was extended to all $a \geq 2$ [13, Thm. 15] to show that for $k \leq 0$, $\bar{\delta}(D_{I,a,k}) \leq 1 - \log 2$. It follows that for $k \leq 0$, $\overline{D}_{I,a,k}$ has a positive lower asymptotic density and, in particular, is infinite. The set $\overline{D}_{I,a,k}$ is also infinite for all $a \geq 2$ and all $k \geq 2$ by [13, Prop. 29]. It is thought that $D_{I,a,k}$ is infinite for all $a \geq 3$ when $k \leq 0$. A partial result in this direction is obtained in [13, Thm. 16]. We point out that although we know $D_{I,2,0}$, the set of $n \geq 1$ such that n divides the central binomial coefficient $\binom{2n}{n}$, is infinite, and has small upper asymptotic

density, it is not known whether it has a positive lower asymptotic density; see the discussion in [13, p. 17].

Moreover, Ballot [13, Thm. 37] showed that for $U(P,Q)$ any regular sequence and for any $a \geq 2$, $D_{U,a,k}$ has asymptotic density 1 for all $k \geq 1$. On the other hand, he showed [13, Thm. 14] that for $k \leq 0$ and U regular and standard ($P^2 \neq 4Q$), the set $D_{U,a,k}$ is finite. Hence, the only hope to find Catalan-like triples for U regular and $k \neq 1$ must occur for $k \geq 2$.

For $U(P,Q)$ regular, all Catalan-like triples are known. There are precisely five such triples with $P > 0$. All are of the shape

$$(U, a, k) = (U(1, Q), a, 2).$$

The first one found is $(U(1,2), 2, 2)$. It was shown in [12, Thm. 3.5] to be the only example with $a = 2$. The others were determined in [13, Thm. 30]; two occur with $a = 4$ ($Q = 2$ and $Q = 3$): one for $a = 6$ and $Q = 5$ and the remaining one for $a = 12$ and $Q = 2$. The regularity hypothesis was made because the search relied on the classification [1, 20] of all regular Lucas sequences U with terms U_n lacking a primitive prime divisor; see also our Sect. 4.5 on primitive divisors. It is an important theorem of [20] that if U is regular, all terms U_n have a primitive prime divisor if $n > 30$. The sequence $U(1,2)$ is outstanding in this respect because it is the only regular sequence having defective[†] terms U_n with $n \geq 13$. If it were not for this sequence, the theorem on primitive prime divisors would hold for $n > 12$ rather than $n > 30$. The question of finding some combinatorial interpretation for the numbers $\frac{1}{U_{n+2}}\binom{2n}{n}_U$, for $U = U(1,2)$, arises, as it does for the four other Catalan-like triples.

It was discovered [13, Thm. 38] that given any triple (U, a, k), U regular, $a \geq 2$, and $k \geq 1$, there exists a minimal positive integer $m = m(U, a, k)$ such that for all $n \geq 1$,

$$\frac{m}{U_{(a-1)n+k}}\binom{an}{n}_U \quad \text{is an integer.}$$

We say the triple (U, a, k) belongs to m. Thus, all triples with $k = 1$ and the five Catalan-like triples belong to $m = 1$. It was found that the triples $(F, 2, 2)$ and $(F, 3, 2)$, resp., belong to $m = 2$ and $m = 3$; see [12, Prop. 3.2 & 4.2] and [13, Rmk. 19].

Integrality proofs used in the papers [12, 13, 69] are arithmetic: They show that for all primes p, the p-adic valuation of say $\binom{2n}{n}$, $\binom{2n}{n}_U$, or $3\binom{3n}{n}_F$ is at least equal to the p-adic valuation of, resp., $n+1$, U_{n+1}, or F_{2n+2}. The p-adic valuation of the terms of Lucas sequences was studied in Sects. 2.4 and 2.5 and for special primes in Sect. 2.12. The p-adic valuation of binomial coefficients

[†] U_n is *defective* if it does not have a primitive prime divisor not dividing D; this notion is entirely different from that of a defective integer m with respect to a sequence X defined in Sect. 4.6.

and Lucasnomials in general is the object of the next section. In particular, a generalized Kummer rule is available to determine the p-adic valuation of Lucasnomials.

5.6 The p-Adic Valuation of Lucasnomials

The p-adic valuation of Lucasnomials $\binom{m+n}{n}_U$, p a regular prime, is amenable to generalized Kummer rules on the one hand. On the other hand, several papers have determined the p-adic valuation of some types of Lucasnomials, mostly Fibonomials, in direct ways.

5.6.1 A Generalized Kummer Rule

We first recall and re-prove Kummer's rule [53].

Suppose p is a prime number. The Kummer rule says that the p-adic valuation of the binomial coefficient $\binom{m+n}{n}$ is the number of carries that occur when adding m and n in base p. For example, to find out the value of $\nu_3\binom{29}{5}$, we execute the base-3 addition of 24 and 5. Since $24 = 2\cdot 9 + 2\cdot 3 = (2,2,0)_3$ and $5 = 1\cdot 3 + 2\cdot 1 = (0,1,2)_3$, this addition generates two carries. Thus, $3^2 \,||\, \binom{29}{5}$. Indeed, $\binom{29}{5} = 3^2\cdot 5\cdot 7\cdot 13\cdot 29$.

Let us prove the Kummer rule. Suppose the base-p expansions of m and n are

$$\begin{aligned} m &= m_\ell p^\ell + m_{\ell-1}p^{\ell-1} + \cdots + m_0, \\ n &= n_\ell p^\ell + n_{\ell-1}p^{\ell-1} + \cdots + n_0, \end{aligned}$$

where all p-ary digits of m and n, m_i and n_i, belong to $[0, p-1]$, and $m_\ell + n_\ell > 0$. Let $i \geq 0$. Then, as one performs, in successive left-to-right columns, the base-p addition of m and n, a nonzero carry $c_i = 1$ occurs between columns i and $i+1$ iff $(m_0 + m_1 p + \cdots + m_i p^i) + (n_0 + n_1 p + \cdots + n_i p^i) \geq p^{i+1}$. That is,

$$c_i = 1 \iff \{\frac{m}{p^{i+1}}\} + \{\frac{n}{p^{i+1}}\} \geq 1. \tag{5.52}$$

On the other hand, using the Legendre formula $\nu_p(N!) = \sum_{i\geq 1}\lfloor \frac{N}{p^i}\rfloor$, we find that

$$\begin{aligned} \nu_p\binom{m+n}{n} &= \nu_p((m+n)!) - \nu_p(m!) - \nu_p(n!) \\ &= \sum_{i\geq 0}\left(\left\lfloor \frac{m+n}{p^{i+1}}\right\rfloor - \left\lfloor \frac{m}{p^{i+1}}\right\rfloor - \left\lfloor \frac{n}{p^{i+1}}\right\rfloor\right). \end{aligned}$$

For two real numbers x and y, the expression $\lfloor x+y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor$ is either 0 or 1. It is 1 if and only if the sum of the fractional parts $\{x\} + \{y\} \geq 1$. Hence,

$$\left\lfloor \frac{m+n}{p^{i+1}} \right\rfloor - \left\lfloor \frac{m}{p^{i+1}} \right\rfloor - \left\lfloor \frac{n}{p^{i+1}} \right\rfloor = 1 \iff \left\{ \frac{m}{p^{i+1}} \right\} + \left\{ \frac{n}{p^{i+1}} \right\} \geq 1.$$

It follows from (5.52) that the p-adic valuation of $\binom{m+n}{n}$ corresponds to the number of carries c_i, $i \geq 0$, in the base-p addition of m and n.

Ward [79] uses a similar reasoning to prove that generalized binomial coefficients with respect to a strongly divisible sequence $X = (x_n)_{n \geq 1}$ are always integers. Define a sequence X of integers to be *regularly divisible* if for any prime p and integer $a \geq 1$ such that p^a divides some term x_n, $n \geq 1$, $p^a \mid x_t$ iff $\rho_a \mid t$, where $\rho_a := \rho(p^a)$ is the rank of p^a in X. If some power p^a of p does not divide any term of X, then we set $\rho_a = \infty$. Ward first proves that a divisible sequence X is strongly divisible if and only if it is regularly divisible. Legendre's formula becomes $\nu_p(x_n x_{n-1} \cdots x_1) = \sum_{a \geq 1} \lfloor n/\rho_a \rfloor$. Since $\binom{m+n}{n}_X$ is an integer iff $\nu_p \binom{m+n}{n}_X \geq 0$ for all primes p, their integrality follows by observing that

$$\left\lfloor \frac{m+n}{\rho_a} \right\rfloor \geq \left\lfloor \frac{m}{\rho_a} \right\rfloor + \left\lfloor \frac{n}{\rho_a} \right\rfloor,$$

for all p and $a \geq 1$.

Knuth and Wilf [52] expanded on the ideas of both Kummer and Ward. In fact, they prove that a sequence X of positive integers is strongly divisible iff X is regularly divisible [52, Prop. 2]. Essentially, the small difference here with Ward's result is that the equivalence is proved without assuming X to be divisible. Knuth and Wilf give Kummer rules for Gaussian coefficients and Fibonomials. We derive below a Kummer rule for general Lucasnomials which is an easy adaptation [11, Sect. 4] of the rule for Fibonomials.

Theorem 82 (The Kummer rule for Lucasnomials) *Let $U(P,Q)$ be a nondegenerate fundamental Lucas sequence and $p \nmid Q$ a prime of rank ρ and rank exponent ν. If p is odd or if PQ is even, then the p-adic valuation of the Lucasnomial $\binom{m+n}{n}_U$ is equal to the number of carries across or to the left of the radix point when adding m/ρ and n/ρ in base p, where a carry across the radix point has weight ν instead of 1. If $p = 2$ and PQ is odd, then the same counting applies except that the weight of a carry between the first and the second place left of the radix point is $\nu_2(P^2 - 3Q)$ instead of 1.*

Remark 32 An alternate wording of Theorem 82 is possible carrying out the addition of m and n in the mixed base $(\ldots, p^{\ell-1}\rho, \ldots, p\rho, \rho, 1)$. Thus, $m = m_\ell p^{\ell-1}\rho + \cdots + m_1\rho + m_0$, where $0 \leq m_0 < \rho$ and $0 \leq m_i < p$ for $i \geq 1$. The advantage is that there are no fractional parts, but the disadvantage is that we are usually less familiar with the use of mixed bases. Of course, a carry

emanating from the initial column is worth ν, and one from the second to the third column is 1 unless $p = 2$ and PQ is odd when it is $\nu_2(P^2 - 3Q)$.

Proof Suppose first p is odd or $p = 2$ and PQ even. Then with the notation $m!_U = U_m U_{m-1} \cdots U_1$, we have, by Theorem 8, a generalized Legendre formula

$$\nu_p(m!_U) = \sum_{i \geq 1} \left\lfloor \frac{m}{\rho(p^i)} \right\rfloor. \tag{5.53}$$

Thus, using Corollaries 11 and 15, we find that

$$\begin{aligned} \nu_p(m!_U) &= \sum_{i=1}^{\nu} \left\lfloor \frac{m}{\rho} \right\rfloor + \sum_{i \geq \nu+1} \left\lfloor \frac{m}{\rho p^{i-\nu}} \right\rfloor \\ &= \nu \left\lfloor \frac{m}{\rho} \right\rfloor + \sum_{i \geq 1} \left\lfloor \frac{m}{\rho p^i} \right\rfloor. \end{aligned}$$

Hence,

$$\begin{aligned} \nu_p \binom{m+n}{n}_U &= \nu \left(\left\lfloor \frac{m+n}{\rho} \right\rfloor - \left\lfloor \frac{m}{\rho} \right\rfloor - \left\lfloor \frac{n}{\rho} \right\rfloor \right) \\ &\quad + \sum_{i \geq 0} \left(\left\lfloor \frac{m/\rho + n/\rho}{p^{i+1}} \right\rfloor - \left\lfloor \frac{m/\rho}{p^{i+1}} \right\rfloor - \left\lfloor \frac{n/\rho}{p^{i+1}} \right\rfloor \right). \end{aligned}$$

The first term on the RHS above is either 0 or ν. It is ν iff $\{m/\rho\} + \{n/\rho\} \geq 1$, i.e., iff a carry occurs over the radix point in the addition of m/ρ and n/ρ in base p. As in the proof of the Kummer rule for binomial coefficients, a carry occurs between columns i and $i+1$ ($i \geq 0$) in the addition of m/ρ and n/ρ iff $\{\frac{m/\rho}{p^{i+1}}\} + \{\frac{n/\rho}{p^{i+1}}\} \geq 1$, which happens whenever

$$\left\lfloor \frac{m/\rho + n/\rho}{p^{i+1}} \right\rfloor - \left\lfloor \frac{m/\rho}{p^{i+1}} \right\rfloor - \left\lfloor \frac{n/\rho}{p^{i+1}} \right\rfloor = 1.$$

A slight hiccup in the above argument occurs when $p = 2$ and PQ is odd. This is explained by Remark 16. Here, $\rho = 3$. Putting $c = \nu_2(P^2 - 3Q)$ and observing that $\rho(2^i) = 6$ for all i, $\nu + 1 \leq i \leq \nu + c$, we see that

$$\begin{aligned} \nu_2(m!_U) &= \sum_{i=1}^{\nu} \left\lfloor \frac{m}{3} \right\rfloor + \sum_{i=\nu+1}^{\nu+c} \left\lfloor \frac{m}{6} \right\rfloor + \sum_{i \geq \nu+c+1} \left\lfloor \frac{m}{6 \cdot 2^{i-\nu-c}} \right\rfloor \\ &= \nu \left\lfloor \frac{m}{3} \right\rfloor + c \left\lfloor \frac{m}{6} \right\rfloor + \sum_{i \geq 1} \left\lfloor \frac{m}{6 \cdot 2^i} \right\rfloor. \end{aligned}$$

Hence,

$$\begin{aligned}
&\nu_2\binom{m+n}{n}_U \\
&\quad = \nu\left(\left\lfloor\frac{m+n}{3}\right\rfloor - \left\lfloor\frac{m}{3}\right\rfloor - \left\lfloor\frac{n}{3}\right\rfloor\right) + c\left(\left\lfloor\frac{m+n}{6}\right\rfloor - \left\lfloor\frac{m}{6}\right\rfloor - \left\lfloor\frac{n}{6}\right\rfloor\right) \\
&\qquad + \sum_{i\geq 0}\left(\left\lfloor\frac{(m/3)+(n/3)}{2^{i+2}}\right\rfloor - \left\lfloor\frac{m/3}{2^{i+2}}\right\rfloor - \left\lfloor\frac{n/3}{2^{i+2}}\right\rfloor\right).
\end{aligned}$$

The quantity $\left\lfloor\frac{m+n}{6}\right\rfloor - \left\lfloor\frac{m}{6}\right\rfloor - \left\lfloor\frac{n}{6}\right\rfloor$ is 1 precisely when a carry occurs between the first and the second digits left of the radix point in the addition of $m/3$ and $n/3$ in base 2. Its weight is c. □

Example 83 Suppose we wish to know the 2-adic valuation of the Fibonomial $\binom{18}{7}_F$. Note that $\rho(2) = 3$, $\nu = 1$, and $\nu_2(P^2 - 3Q) = 2$. A direct calculation using Theorems 8 and 14 gives

$$\binom{18}{7}_F \sim \frac{F_{18}\cdots F_{12}}{7!_F} \sim \frac{F_{12}F_{15}F_{18}}{F_3F_6} \quad \text{(base 2)}.$$

Now $\nu_2(F_{12}F_{15}F_{18}) = (1 + \nu_2(F_6)) + (0 + \nu_2(F_3)) + (0 + \nu_2(F_6)) = 4 + 1 + 3 = 8$, while $\nu_2(F_3F_6) = 1 + 3 = 4$. Thus, $\nu_2\binom{18}{7}_F$ is the difference $8 - 4 = 4$. Using Theorem 82, we need to add $11/3$ and $7/3$ in base 2. Since $11/3 = (1,0,0,1)_2 + 2/3$ and $7/3 = (0,0,1,0)_2 + 1/3$, we see that there is a carry across the radix point as $2/3 + 1/3 = 1 \geq 1$ which creates another two in the first two places left of this point. So we find three carries with the middle one worth 2. Alternatively, using Remark 32, in the mixed base $(\ldots, p\rho, \rho, 1) = (\ldots, 6, 3, 1)$, we have $11 = 6 + 3 + 2 = (1,1,2)$ and $7 = 6 + 1 = (1,0,1)$. There are again three carries, and the second one has a weight of 2. □

Application 84 Let us use an arithmetic argument to prove that the Fibonomial Catalan number $C_F(n) = \frac{1}{F_{n+1}}\binom{2n}{n}_F$ $(n \geq 0)$ is an integer. If $C_F(n)$ is a non-integral rational number, there must exist a prime p for which its valuation is negative. Since $\binom{2n}{n}_F$ is an integer, p must divide F_{n+1}. Thus, by Theorem 8, there is a positive integer λ such that $n + 1 = \lambda p^e \rho$, where $\rho = \rho(p)$, $e \geq 0$, and $p \nmid \lambda$. By Lemmas 11 and 13, we see that

$$\nu_p(F_{n+1}) = \begin{cases} \nu + e, & \text{if } p \text{ is odd;} \\ \nu + ((e-1) + c)\cdot[e \geq 1], & \text{if } p = 2, \end{cases}$$

where again ν is the rank exponent of p and here, since $F = U(1,-1)$, $c = \nu_2(P^2 - 3Q) = \nu_2(4) = 2$. To find out the p-adic valuation of $\binom{2n}{n}_F$, we add n/ρ to itself in base p and count carries according to Theorem 82. Since

$$\frac{n}{\rho} = \lambda p^e - \frac{1}{\rho} = (\lambda p^e - 1) + \frac{\rho - 1}{\rho},$$

we see that the e least significant p-ary digits of $\lambda p^e - 1$ are all $p-1$ and that the fractional part of n/ρ is $(\rho-1)/\rho \geq 1/2$. Hence, this addition produces at least $e+1$ carries. By Theorem 82, these carries imply that

$$\nu_p \binom{2n}{n}_F \geq \begin{cases} \nu + e, & \text{if } p \text{ is odd;} \\ \nu + ((e-1)+c) \cdot [e \geq 1], & \text{if } p = 2. \end{cases}$$

Hence, $\nu_p \binom{2n}{n}_F \geq \nu_p(F_{n+1})$ and $\nu_p(C_F(n)) \geq 0$. This is a contradiction. □

Remark 33 The same argument as in the above application would show that the p-adic valuation of a Lucasnomial Catalan number $C_U(n)$ is nonnegative if $p \nmid Q$. If $p \mid Q$ and $p \nmid P$, then by Lemma 6, no term of U is divisible by p. In this case, $\nu_p(C_U(n)) = 0$. It remains to evaluate $\nu_p(C_U(n))$ when p is a special prime, i.e., when $p \mid \gcd(P, Q)$. When p is special, then Theorem 46 describes $\nu_p(U_n)$ for all $n \geq 1$. It is then possible to evaluate the p-adic valuation of any generalized Lucasnomial Fuss-Catalan number $C_{U,a,r}(n)$; see (5.44) for their definition. It was shown in the proof of [15, Thm. 6] that this valuation is always nonnegative. In particular, $\nu_p(C_U(n)) \geq 0$ if $p \mid \gcd(P, Q)$.

There is no Kummer rule for evaluating the p-adic valuation of Lucasnomials when p is special, so an explicit description was given in [15, Thm. 1]. The main ingredient of the proof was Theorem 46. We restate the result below.

Suppose $U = U(P, Q)$, where $P = p^a P'$, $Q = p^b Q'$, p is a prime, a and b are positive, and $p \nmid P'Q'$. Let m and n be positive integers and r_m and r_n be the respective remainders of the Euclidean divisions of m and of n by $2p$. Then the next theorem holds.

Theorem 85 *The p-adic valuation of the Lucasnomial $\binom{m+n}{n}_U$ is*

$$\begin{cases} amn + \nu_p \binom{m+n}{n}_{U'} \cdot [b = 2a], & \text{if } b \geq 2a; \\ b\lfloor \frac{mn}{2} \rfloor + \nu_p \binom{\lfloor \frac{m+n}{2} \rfloor}{\lfloor \frac{n}{2} \rfloor} + \left(a + \nu_p\left(\frac{m+1}{2}\right)\right) \cdot [\mathcal{P}_1] + c' \cdot [\mathcal{P}_2], & \text{if } b < 2a, \end{cases}$$

where U' is the Lucas sequence $U(P', Q')$, $c' = \nu_p(P'^2 - Q')$, $[-]$ denotes as usual the Iverson symbol, and $\mathcal{P}_1$ and $\mathcal{P}_2$ are the following conditions:

- $\mathcal{P}_1$: *m and n are odd.*
- $\mathcal{P}_2$: *$2 \leq p \leq 3$ and $2a = b + 1$ and $r_m + r_n \geq 2p$.*

Note that $\nu_p \binom{m+n}{n}_{U'}$ can be evaluated using the Kummer rule for Lucasnomials as $p \nmid Q'$. Concrete examples of calculations using Theorem 85 can be found in [15, Sect. 3].

5.6.2 A Generalized Legendre Formula

We provide a generalization to Lucas factorials $n!_U$ of the Legendre formula

$$\nu_p(n!) = \sum_{k\geq 1} \left\lfloor \frac{m}{p^k} \right\rfloor = \frac{n - s_p(n)}{p-1}, \tag{5.54}$$

where $s_p(n)$ is the sum of the p-ary digits of n.

Theorem 86 *Let $p \nmid Q$ be a prime. If $p = 2$, we assume additionally that P is even or $Q \equiv 1 \pmod 4$. Suppose p has rank ρ and rank exponent ν in U; then, for all $n \geq 1$, we have*

$$\nu_p(n!_U) = \sum_{k\geq 1} \left\lfloor \frac{n}{\rho_k} \right\rfloor = (\nu - 1)\left\lfloor \frac{n}{\rho} \right\rfloor + \frac{p\lfloor n/\rho \rfloor - s_p(\lfloor n/\rho \rfloor)}{p-1}, \tag{5.55}$$

where ρ_k is the rank of p^k in U and s_p is the base-p sum-of-digit function.

Proof Suppose $n = a_\ell p^{\ell-1}\rho + \cdots + a_1\rho + a_0$, where $0 \leq a_0 < \rho$ and $0 \leq a_i < p$ for $i \geq 1$. Then, as seen at the beginning of the proof of Theorem 82,

$$\begin{aligned} \nu_p(n!_U) &= \nu\left\lfloor \frac{n}{\rho} \right\rfloor + \sum_{k\geq 1} \left\lfloor \frac{n}{\rho p^k} \right\rfloor \\ &= (\nu - 1)\left\lfloor \frac{n}{\rho} \right\rfloor + \sum_{k\geq 0} \left\lfloor \frac{n}{\rho p^k} \right\rfloor. \end{aligned}$$

But, as $\lfloor n/\rho p^k \rfloor = \sum_{i=k}^{\ell-1} a_{i+1} p^{i-k}$, we find that

$$\begin{aligned} \sum_{k\geq 0} \left\lfloor \frac{n}{\rho p^k} \right\rfloor &= \sum_{k=0}^{\ell-1} \sum_{i=k}^{\ell-1} a_{i+1} p^{i-k} \\ &= \sum_{i=0}^{\ell-1} a_{i+1} \sum_{k=0}^{i} p^{i-k} = \sum_{i=0}^{\ell-1} a_{i+1} \sum_{u=0}^{i} p^u \\ &= \sum_{i=0}^{\ell-1} a_{i+1} \frac{p^{i+1}-1}{p-1} = \frac{1}{p-1}\big(p\lfloor n/\rho \rfloor - s_p(\lfloor n/\rho \rfloor)\big), \end{aligned}$$

which proves the result. □

Note that if $U = U(2,1)$, then for all primes p, we get $\rho = p$ and $\nu = 1$. Moreover, if $n = \sum_{i=0}^{\ell} a_i p^i$, then $p\lfloor n/\rho \rfloor = n - a_0$ and $s_p(\lfloor n/\rho \rfloor) = s_p(n) - a_0$. Hence, if we apply (5.55) to $U(2,1)$, we recover (5.54).

If $p = 2$, P is odd, and $Q \equiv -1 \pmod 4$, then $c = \nu_2(P^2 - 3Q) \geq 2$, and, as observed in Remark 16, the law of repetition applies not from $\rho = 3$, but from $p\rho = 6$. That is, $\nu_2(U_{6n}) = \nu_2(U_6) + \nu_2(n)$ and $\nu_2(U_6) - \nu_2(U_3) = c > 1$. As seen at the end of the proof of Theorem 82, we have

$$\nu_2(n!_U) = \nu\left\lfloor \frac{n}{3} \right\rfloor + (c-1)\left\lfloor \frac{n}{6} \right\rfloor + \sum_{k\geq 0} \left\lfloor \frac{n}{6 \cdot 2^k} \right\rfloor.$$

Since P is odd and $Q \equiv -1 \pmod 4$, $U_3 = P^2 - Q \equiv 2 \pmod 4$ so that $\nu = 1$. If $n = a_0 + a_1 3 + a_2 6 + a_3 12 + \cdots + a_\ell 3 \cdot 2^{\ell-1}$, then $\sum_{k=0}^{\ell-2} \lfloor n/(6 \cdot 2^k) \rfloor = \sum_{k=0}^{\ell-2} \sum_{i=k}^{\ell-2} a_{i+2} 2^{i-k}$. Inverting the order of summation as we did in the proof of Theorem 86, we obtain the following complement to Theorem 86, namely, the equation

$$\begin{aligned} \nu_2(n!_U) &= \left\lfloor \frac{n}{3} \right\rfloor + (c-1) \left\lfloor \frac{n}{6} \right\rfloor + \Big(\lfloor n/3 \rfloor - s_2(\lfloor n/3 \rfloor) \Big) \\ &= 2 \times \left\lfloor \frac{n}{3} \right\rfloor + (c-1) \left\lfloor \frac{n}{6} \right\rfloor - s_2\left(\left\lfloor \frac{n}{3} \right\rfloor \right). \end{aligned} \tag{5.56}$$

For example, using (5.56) for $F = U(1, -1)$, we find that $c = 2$ and

$$\nu_2(100!_F) = 2 \times 33 + 1 \times 16 - s_2(32 + 1) = 66 + 16 - 2 = 80.$$

Remark 34 The two formulas (5.55) and (5.56) should coincide if $p = 2$, P is odd, and $Q \equiv 1 \pmod 4$. In this case, because $c = 1$, both analyses are valid provided we take into account that $\nu = \nu_2(P^2 - Q) \geq 2$. Thus, they coincide if we replace the coefficient of $\lfloor n/3 \rfloor$ by $\nu + 1$ instead of 2 in (5.56).

Remark 35 If for the Fibonacci sequence, the generalized Legendre formula (5.56) yields

$$\nu_2(n!_F) = 2\lfloor n/3 \rfloor + \lfloor n/6 \rfloor - s_2(\lfloor n/3 \rfloor),$$

Phunphayap and Pongsriiam [67, eq. (9)] obtained another expression by a direct calculation based on the 2-adic valuation of Fibonacci terms, namely,

$$\nu_2(n!_F) = \lfloor (n+3)/6 \rfloor + 3\lfloor n/6 \rfloor + \nu_2(\lfloor n/6 \rfloor !).$$

5.6.3 Explicit Valuations

As seen in Example 83, calculating the valuation of a Lucasnomial can be done directly or by using the Kummer rule for Lucasnomials.

Several papers [58–61, 67, 68] have studied the p-adic valuation of some Fibonomial coefficients in a direct manner. We note in passing that, using similar methods, results for general Lucasnomials can surely be achieved. The paper [11] used the Kummer rule (Theorem 82) to improve upon Fibonomial results of the papers [58–61], but also included valuation theorems for general Lucasnomials. The proofs were often much shorter. However, the papers [67, 68] established the p-adic valuation of larger collections of Fibonomials than in any preceding papers using direct elementary methods.

For $n \geq 1$ an integer and p a prime, we have $\binom{pn}{n} = p\binom{pn-1}{n-1}$. Hence, p divides $\binom{pn}{n}$ for all $n \geq 1$. It is easy to see that $p \mid \binom{sn}{n}$ for all $n \geq 1$ if and only

if $p \mid s$. Marques et al., who initiated these studies, posed two corresponding Fibonomial questions:

1. Given a prime p, when does p divide $\binom{pn}{n}_F$?
2. What necessary and sufficient condition must s satisfy in order for p to divide all Fibonomials of the type $\binom{sn}{n}_F$?

In [58], the authors proved that $2 \mid \binom{2n}{n}_F$ iff $n \geq 2$. It is re-proved in a few lines in [11, Thm 3.1] using the Kummer rule. For $p = 2$, the answer to Question **2** is that $6 \mid s$. The case $p = 3$ is solved in [59]. The prime 3 divides $\binom{3n}{n}_F$ iff $n \geq 2$ and $n \neq 2 \cdot 3^k$, $(k \geq 0)$. The set of exceptions is slim and is made to appear naturally by using the Kummer rule in a short proof [11, Thm. 1.1]. As for Question **2**, s must be divisible by 12 [59, Thm. 2]. The case $p = 5$ is peculiar since $\nu_5(F_n) = \nu_5(n)$ for all $n \geq 1$. Thus, $\binom{m}{n}$ and $\binom{m}{n}_F$ have the same 5-valuation. In particular, Question **1** has an affirmative answer for all $n \geq 1$. The use of the Kummer rule was tested on the case $p = 7$ in [11, Thm. 3.6], but the proof was notably longer. Although the set of integers n for which $7 \nmid \binom{7n}{n}_F$ was explicitly described, it necessitated three parameters. Instead of going further along this method, it was shown that, given a prime p, the set of integers $n \leq x$ for which $p \nmid \binom{pn}{n}_F$ is $O(\log^s x)$, where s is a nonnegative integer $\leq p-2$. In other words, divisibility of $\binom{pn}{n}_F$ by p occurs on a set of asymptotic density 1. The remark was made that the same result holds if F is replaced by any Lucas sequence U. Marques et al. [61] took $n = p^a$, $(a \geq 1)$, and found that if $p \equiv \pm 2 \pmod 5$, then p divides $\binom{pn}{n}_F$; they conjectured $p \nmid \binom{pn}{n}_F$ whenever $p \equiv \pm 1 \pmod 5$. The conjecture was proved in [60], but also in [11, Thm. 2.1] with a short proof that used the Kummer rule. In [60], the authors also found the exact valuation of $\binom{p^{a+1}}{p^a}_F$ for $p \equiv \pm 2 \pmod 5$. (Their result is only accurate for primes whose rank exponent is 1 or for even exponents a.) Theorem 7.1 of [11] gave the complete p-adic valuation of the Lucasnomials $\binom{p^b}{p^a}_U$ for all $U = U(P, Q)$ and all primes $p \nmid Q$, $0 \leq a < b$. This was done using the Kummer rule for Lucasnomials. Question **2** was addressed not only for the Fibonacci case but for any Lucas sequence U in [11, Thm. 6.1]: p divides $\binom{sn}{n}_U$ for all $n \geq 1$ iff $\operatorname{lcm}(p, \rho) \mid s$, where ρ is the rank of p in U. Thus, if $p \nmid D = P^2 - 4Q$, then the condition on s is that $p\rho$ divides s.

Phunphayap and Pongsriiam [67] managed by direct elementary methods to find explicit p-adic valuation formulas for all Fibonomials of the form $\binom{\ell_1 p^b}{\ell_2 p^a}_F$, where $b \geq a \geq 1$ and ℓ_1 and ℓ_2 are positive integers. Assume $\ell_1 p^b > \ell_2 p^a$, and define s and r as the respective remainders of the Euclidean divisions of $\ell_1 p^b$ and $\ell_2 p^a$ by ρ, the rank of p. Theorem 13 of [67] gives for primes $p \equiv \pm 2 \pmod 5$ six separate formulas depending on the relative sizes of r and s and on the divisibility of ℓ_1 and ℓ_2 by ρ. But for primes $p \equiv \pm 1 \pmod 5$, they find a single formula, which we give here

$$\nu_p\binom{\ell_1 p^b}{\ell_2 p^a}_F = \nu_p\binom{m}{k} + [r < s] \cdot \big(a + \nu + \nu_p(m-k)\big), \tag{5.57}$$

where $m = \lfloor \frac{\ell_1 p^{b-a}}{\rho} \rfloor$, $k = \lfloor \frac{\ell_2}{\rho} \rfloor$, and ν is the rank exponent of p in F. It was shown [11, Thm. 7.1] that the p-adic valuation of a Lucasnomial of the shape $\binom{p^b}{p^a}_U$, $(b \geq a \geq 0)$, is 0 if $\rho \mid p-1$ (and, incidentally, if $b \equiv a \pmod 2$, when $\rho \mid p+1$). Suppose $U = F$, $p \equiv \pm 1 \pmod 5$, and $0 < a < b$. Then $\rho \mid p-1$ by Theorem 9. Thus, ρ divides $p^a - 1$ and $p^b - 1$. Hence, $r = s = 1$. Choosing $\ell_1 = \ell_2 = 1$, we see that $k = 0$. Therefore, we indeed recover from Equation (5.57) the fact that $\nu_p\binom{p^b}{p^a}_F = 0$. Actually, we see from (5.57) that, for $p \equiv \pm 1 \pmod 5$, $\nu_p\binom{\ell p^b}{p^a}_F = 0$ $(0 < a < b)$ as soon as $\rho \nmid \ell$. Indeed, $\rho \nmid \ell$ implies $r \geq 1 = s$. Moreover, with $\ell_2 = 1$, we obtain $k = 0$.

In [68], given any prime p, the same two authors find formulas for the p-adic valuation of the Fibonomials $\binom{p^a n}{n}_F$, where $a \geq 1$ is an integer. As an example, for $p \equiv \pm 2 \pmod 5$, $p \neq 2$, a even, this valuation is

$$\frac{A}{p-1} - \frac{a}{2} \cdot [s \neq 0] - \nu_p(A!),$$

where $s = (n \pmod \rho)$, $A = \lfloor m(p^a - 1)/\rho \rfloor$, and $m = n/p^{\nu_p(n)}$. In some corollaries of their results, they are able to determine, given some p^a, the set of integers n for which p divides $\binom{p^a n}{n}_F$, a problem which extends Question **1**. For instance, they find that $\binom{2^3 n}{n}_F$ is odd if and only if n is of the form $(1 + 6 \cdot 8^k)/7$, $k \geq 0$.

Knowing the p-adic valuation of a Lucasnomial is zero should not prevent us from finding its residues modulo powers of p. (See in particular Sect. 5.8).

In [29], the authors prove a result for specific Fibonomials, namely

$$\binom{p^{a+1}}{p^a}_F \equiv 1 + p + p^2 \pmod{p^3},$$

for all primes $p \equiv \pm 1 \pmod 5$ whose rank in the Fibonacci sequence is $p-1$ and all $a \geq 3$.

5.7 Lucas' Congruence

Let p be a prime and $B = (b_{i,j})_{0 \leq i,j \leq p-1}$ be the $p \times p$ matrix of binomial coefficient $b_{i,j} = (\binom{i}{j} \pmod p)$. For instance, if $p = 3$, then

$$B = \begin{matrix} 1\,0\,0 \\ 1\,1\,0 \\ 1\,2\,1 \end{matrix}$$

Then the first $4p$ lines of Pascal's triangle modulo p are

$$\begin{array}{l} B \\ B\ B \\ B\ (2B)\ B \\ B\ (3B)\ (3B)\ B \\ \ldots \end{array}$$

where multiplication is taken modulo p.

In his classical memoir on Lucas sequences [56, p. 229], Lucas showed how constructing the Pascal triangle modulo a prime p lets the initial first p lines reappear further down the triangle but flanked with binomial coefficients and deduced from this structure the now-famous congruence for binomial coefficients modulo p.

Theorem 87 *If p is a prime number and m and n are two nonnegative integers, then Lucas' congruence*

$$\binom{m}{n} \equiv \prod_{i \geq 0} \binom{m_i}{n_i} \pmod{p}$$

holds, where $0 \leq m_i, n_i < p$ are the ith p-ary digits of m and n (see Sect. 5.6.1).

Meštrović wrote a thorough compendium [63] of the various proofs, extensions, and applications of Lucas' theorem that appeared in the literature up until 2014. Section 5 of [63] is dedicated to the generalizations of Lucas' theorem which have to do with generalized binomial coefficients, including Lucasnomials.

These days, the short formal proof of Lucas' theorem given by Fine [26] is perhaps the most often reproduced. It appears on the Wikipedia page on Lucas' theorem or on page 6 of Meštrović's paper [63]. It is often noted that if

$$\binom{mp+s}{np+t} \equiv \binom{m}{n}\binom{s}{t} \pmod{p}, \tag{5.58}$$

where m, n, s, and t are nonnegative integers with s and t less than p, then Theorem 87 holds. Thus, we may also prove Lucas' congruence by noting that

$$(1+x)^{mp+s} = \left((1+x)^p\right)^m (1+x)^s \equiv (1+x^p)^m (1+x)^s \pmod{p}.$$

Thus, if $[x^k]f(x)$ denotes the coefficient of x^k in the polynomial $f(x)$, because s and t are less than p, we see that

$$[x^{np+t}](1+x)^{mp+s} \equiv [x^{np}](1+x^p)^m \cdot [x^t](1+x)^s$$
$$= \binom{m}{n}\binom{s}{t} \pmod{p}.$$

Hence, (5.58) follows.

There are generalizations of Lucas' theorem—e.g., modulo higher powers of primes—which may themselves admit extensions to Lucasnomials. In this section, we limit ourselves to some of the attempts at generalizing the Lucas congruence (as it is) to Lucasnomials. Our material overlaps much of Meštrović's [63, Sect. 5]. However, the presentation differs, a more uniform notation is used, some post-2014 references are cited, and a few remarks and improvements on existing results have been added.

As usual, historically, the first attempts started with q-binomial coefficients and Fibonomials. In 1965, Olive [65] obtained the polynomial congruence

$$\binom{md+s}{nd+t}_q \equiv \binom{m}{n}\binom{s}{t}_q \pmod{\Phi_d(q)}, \tag{5.59}$$

which is a q-analogue of (5.58), where d is a positive integer and $\Phi_d(q)$ the dth cyclotomic polynomial (mentioned in Sects. 3.5 and 4.3). Note that if d is a prime p, then the irreducible polynomial $\Phi_p(q)$ is the usual q-analogue of the rational prime p. Also if $d = p$, we recover (5.58) by letting q tend to 1. Thus, (5.59) is a true generalization of Lucas' congruence. As with many Gaussian coefficient congruences, their consequences and applications in terms of Lucas sequences await examination. In 1967, Fray [27, Thm. 3.11] gave the following generalization of (5.58):

$$\binom{m\rho+s}{n\rho+t}_q \equiv \binom{m}{n}\binom{s}{t}_q \pmod{p}, \tag{5.60}$$

where q was viewed as a *p-integral rational number*, i.e., a rational number with both numerator and denominator prime to p, ρ is the order of q modulo p, and m, n, s, and t are nonnegative integers with s and $t < \rho$.

The Fibonomial triangle is obtained by replacing the binomial coefficient $\binom{n}{k}$ in Pascal's triangle with the Fibonomial $\binom{n}{k}_F$. Interest in the Fibonomial triangle modulo primes began in the 1960s (see for instance [37]) and flourished in the 1990s [23, 24, 38, 74, 82, 83], often with the intention of discovering an analogue of Lucas' theorem. This study was frequently limited to the primes 2, 3, or 7 or to primes p satisfying some particular condition. However, Wilson [83], on the one hand, and Wells [82] and Holte [38], on the other, found analogues of (5.58) that worked for general primes. Wilson showed that for a prime p not 2, nor 5, we have

$$\binom{m\rho+s}{n\rho+t}_F \equiv \binom{m}{n}\binom{s}{t}_F F_{\rho+1}^e \pmod{p}, \tag{5.61}$$

where $e = (n\rho+t)(m-n) + n(s-t)$.

In 2001, Hu and Sun [41] found a general Lucasnomial extension of Lucas' theorem that subsumes several of the previous results, in particular the q-analogue (5.60) of Fray and the Fibonomial analogue of Wilson (5.61).

Theorem 88 *Suppose $U(P,Q)$ is a regular and nondegenerate Lucas sequence. If q is a positive integer, then*

$$\binom{mq+s}{nq+t}_U \equiv \binom{m}{n}\binom{s}{t}_U U_{q+1}^e \pmod{P_q}, \tag{5.62}$$

where m, n, s, and t are nonnegative integers, s and t are less than q, e is $(nq+t)(m-n)+n(s-t)$, and P_q is the largest primitive factor of U_q. If q or e is even, then the factor U_{q+1}^e in (5.62) can be replaced by $(-1)^{(mt-ns)(q-1)}Q^{eq/2}$.

One easily checks that

$$e \equiv \begin{cases} mt-sn, & \text{if } q \text{ is even;} \\ mt-sn+n(m-n), & \text{if } q \text{ is odd;} \end{cases} \pmod 2. \tag{5.63}$$

By Corollary 39, requiring that $U(P,Q)$ be nondegenerate when P and Q are coprime comes down to discarding the two sequences $U(\pm 1,1)$. If $(P,Q) = (2,1)$ and q is a prime, then $P_q = U_q = q$ and $U_{q+1} = q+1 \equiv 1 \pmod q$. This shows that (5.62) is indeed a generalization of (5.58). It clearly extends the result of Wilson, since taking $U = F$ and $q = \rho$, we have $p \mid P_q$. To see that it generalizes (5.60), assume q is a p-integral rational number of order ρ modulo p. Then we find that

$$\frac{q^{\rho+1}-1}{q-1} = \frac{q^{\rho+1}-q^\rho+q^\rho-1}{q-1} = q^\rho + \frac{q^\rho-1}{q-1} \equiv 1+0 = 1 \pmod p.$$

Hence, $U_{\rho+1}^e \equiv 1 \pmod p$.

If p is a primitive prime factor of U_q, then (5.62) holds modulo p^ν since the rank ρ of p is q and ν is the rank exponent of p. Hence, for all primes $p \nmid Q$, we find that

$$\binom{m\rho+s}{n\rho+t}_U \equiv \binom{m}{n}\binom{s}{t}_U U_{\rho+1}^e \pmod{p^\nu}. \tag{5.64}$$

Since $2U_{\rho+1} = U_\rho V_1 + U_1 V_\rho$, we see that, for p odd, we also have

$$\binom{m\rho+s}{n\rho+t}_U \equiv \binom{m}{n}\binom{s}{t}_U (V_\rho/2)^e \pmod{p^\nu}. \tag{5.65}$$

Remark 36 The congruences (5.64) and (5.65) hold without the hypothesis of Theorem 88 that U be regular. (The proof of Theorem 88 requires in [41, Lemma 4] that U_q and U_{q+1} be coprime. However, if $p \nmid Q$, then we know by

Lemma 7 that $p \nmid \gcd(U_q, U_{q+1})$, which suffices for the congruence to hold modulo p, or p^ν, when $q = \rho(p)$.)

Congruence (5.58) is equivalent to Lucas' theorem, but the existence of Lucasnomial generalizations of this congruence does not usually imply the wishful generalization of Lucas' theorem:

$$\binom{m}{n}_U \equiv \prod_{i\geq 0} \binom{m_i}{n_i}_U \pmod{p}, \tag{5.66}$$

where the m_i and n_i are the digits of m and n in the mixed base described in Remark 32. For instance, the Fibonomial $\binom{5}{1}_F = F_5 = 5 \equiv 2 \pmod 3$, but as $\rho_F(3) = 4$, we have $5 = 1 \cdot \rho + 1$, $1 = 0 \cdot \rho + 1$, and $\binom{1}{0}_F \binom{1}{1}_F = 1$. However, in this regard, we do have a couple of corollaries to Theorem 88.

Corollary 89 Let $U(P, Q)$ be a fundamental Lucas sequence, and let $p \nmid Q$ be a prime of rank ρ in U. Then, for all m and n nonnegative integers, we have

$$p \text{ divides } \binom{m}{n}_U \iff p \text{ divides } \prod_{i\geq 1} \binom{m_i}{n_i} \cdot \binom{m_0}{n_0}_U,$$

where $(m_i)_{i\geq 0}$ and $(n_i)_{i\geq 0}$ are the respective digits of m and n in the mixed base $(1, \rho, p\rho, \ldots, p^i\rho, \ldots)$. □

Proof By (5.64), we have

$$\binom{m}{n}_U \equiv \binom{\lfloor m/\rho \rfloor}{\lfloor n/\rho \rfloor} \binom{m_0}{n_0}_U U_{\rho+1}^e \pmod{p}.$$

By Lucas' theorem,

$$\binom{\lfloor m/\rho \rfloor}{\lfloor n/\rho \rfloor} \equiv \prod_{i\geq 1} \binom{m_i}{n_i} \pmod{p}.$$

The corollary follows because, by Lemma 7, $p \nmid U_{\rho+1}$ since $p \mid U_\rho$. □

From Corollary 89, we easily deduce the following result.

Corollary 90 Let $U(P, Q)$ be a fundamental Lucas sequence and $p \nmid Q$ a prime of rank $\rho \geq p$. Then, for all m and n nonnegative integers, we have

$$p \text{ divides } \binom{m}{n}_U \iff p \text{ divides } \prod_{i\geq 0} \binom{m_i}{n_i}_U,$$

where $(m_i)_{i\geq 0}$ and $(n_i)_{i\geq 0}$ are the respective digits of m and n in the mixed base $(1, \rho, p\rho, \ldots, p^i\rho, \ldots)$. □

Proof By Corollary 89, it suffices to check that for each $i \geq 1$, $p \mid \binom{m_i}{n_i}$ iff $p \mid \binom{m_i}{n_i}_U$. But, for $i \geq 1$, we have $0 \leq m_i, n_i < p$. Thus, $p \mid \binom{m_i}{n_i}$ iff $m_i < n_i$. By the Kummer rule for Lucasnomials (Theorem 82), $p \mid \binom{m_i}{n_i}_U$ iff either $m_i < n_i$, or $m_i \geq n_i$ and $\{(m_i - n_i)/\rho\} + \{n_i/\rho\} \geq 1$. But the latter condition holds iff $\lfloor m_i/\rho \rfloor - \lfloor (m_i - n_i)/\rho \rfloor - \lfloor n_i/\rho \rfloor = 1$ and that cannot happen since $\rho \geq p$ entails that each of the three integral parts is zero. □

We observe that Corollaries 89 and 90 imply the naive version of Lucas' theorem (5.66) for $p = 2$, since the rank of 2 in U is either 2 or 3. Thus, if Q is odd, then

$$\binom{m}{n}_U \equiv \prod_{i \geq 0} \binom{m_i}{n_i}_U \pmod 2, \tag{5.67}$$

where as before the m_i and n_i are the digits of m and n in the mixed base $(1, \rho, 2\rho, \ldots, 2^i\rho, \ldots)$.

In the proof of Corollary 90, we saw that for $i \geq 1$, $p \mid \binom{m_i}{n_i}$ implies $p \mid \binom{m_i}{n_i}_U$. This implication holds even if $\rho < p$. Thus, with Corollary 89, we see that the divisibility of $\prod_{i \geq 1} \binom{m_i}{n_i}_U$ by p is a necessary condition for p to divide $\binom{m}{n}_U$. That is, we at least have the following result:

Corollary 91 Let $U(P, Q)$ be a fundamental Lucas sequence and $p \nmid Q$ be a prime of rank ρ. Then, for all m and n nonnegative integers, we have

$$p \text{ divides } \binom{m}{n}_U \implies p \text{ divides } \prod_{i \geq 0} \binom{m_i}{n_i}_U,$$

where $(m_i)_{i \geq 0}$ and $(n_i)_{i \geq 0}$ are the respective digits of m and n in the mixed base $(1, \rho, p\rho, \ldots, p^i\rho, \ldots)$. □

The congruence (5.67) appeared in the 2014 paper [23] as Theorem 3.4 at least when U is the Fibonacci sequence. The authors checked the congruence via a case-by-case use of the Kummer rule for Fibonomials.

In 2016, Southwick [74] conjectured Corollary 90 again in the context of the Fibonacci sequence. In 2018, Debellevue and Kryuchkova [24] worked out a direct proof of Southwick's conjecture using the Kummer rule for Fibonomials; i.e., they did not see it as a consequence of Theorem 88. Their main theorem, [24, Thm. 4.6], states that if p is an odd prime of rank $\rho = p + 1$ in the Fibonacci sequence, then

$$\binom{mp^a\rho + s}{np^a\rho + t}_F \equiv \binom{m}{n}\binom{s}{t}_F (-1)^{mt - sn} \pmod p, \tag{5.68}$$

where $a \geq 0$, $0 < s < p^a\rho$, $0 \leq t < p^a\rho$, and $0 \leq m, n < p$. This congruence has nice consequences for the structure of the Fibonomial triangle modulo such a prime, since blocks of size $p^a\rho$ reappear flanked by binomial coefficients further down the triangle just as Lucas discovered they did in the case of the

Pascal triangle, only up to a possible -1 factor this time. With sharp eyes or a magnifying glass, one can see the Fibonomial triangle modulo 7 in [24, Fig. 1].

We provide next a theorem which shows that the same phenomenon holds in broader generality.

Theorem 92 *Suppose $U(P,Q)$ is a fundamental Lucas sequence with $Q = \pm 1$ and p is an odd prime whose rank ρ is even ($\rho = 2\rho_V$). Assume a, m, n, s, and t are nonnegative integers with s and t less than $p^a\rho$. Then*

$$\binom{mp^a\rho + s}{np^a\rho + t}_U \equiv \binom{m}{n}\binom{s}{t}_U \epsilon_{m,n,s,t} \pmod{p}.$$

where

$$\epsilon_{m,n,s,t} = \begin{cases} (-1)^{mt-sn}, & \text{if } 4 \mid \rho \text{ or } Q = 1; \\ 1, & \text{if } 2 \,||\, \rho \text{ and } Q = -1. \end{cases}$$

Proof Suppose first $Q = -1$. Note that when applying Theorem 88 to the Lucasnomial $\binom{mq+s}{nq+t}_U$ with $q = \rho$, we may, since $Q = -1$ and ρ is even, using (5.63), replace $U^e_{\rho+1}$ by $(-1)^{mt-sn}(-1)^{e\rho_V} = (-1)^{(mt-sn)(1+\rho_V)}$. Write $s = s'\rho + s_0$ and $t = t'\rho + t_0$, where $0 \le s_0, t_0 < \rho$. Using Hu and Sun's theorem with $q = \rho$ a couple of times and Lucas' theorem, we find that

$$\begin{aligned} \binom{mp^a\rho + s}{np^a\rho + t}_U &= \binom{(mp^a + s')\rho + s_0}{(np^a + t')\rho + t_0}_U \equiv \binom{mp^a + s'}{np^a + t'}\binom{s_0}{t_0}_U (-1)^x \\ &\equiv \binom{m}{n}\binom{s'}{t'}\binom{s_0}{t_0}_U (-1)^x \equiv \binom{m}{n}\binom{s'\rho + s_0}{t'\rho + t_0}_U (-1)^{x+y} \\ &= \binom{m}{n}\binom{s}{t}_U (-1)^{x+y} \pmod{p}, \end{aligned}$$

where

$$\begin{aligned} x &= ((m + s')t_0 - s_0(n + t'))(1 + \rho_V) \\ y &= (s't_0 - s_0t')(1 + \rho_V). \end{aligned}$$

$$\begin{aligned} \text{Hence,} \qquad x + y &= \big((m + s')t_0 - s_0(n + t') + (s't_0 - s_0t')\big)\big(1 + \rho_V\big) \\ &\equiv (mt_0 - s_0n)(1 + \rho_V) \equiv (mt - sn)(1 + \rho_V) \pmod{2}, \end{aligned}$$

where the justification for the latter congruence is that, ρ being even, $t \equiv t_0 \pmod 2$ and $s \equiv s_0 \pmod 2$. Thus,

$$(-1)^{x+y} = \begin{cases} (-1)^{mt-sn}, & \text{if } 4 \mid \rho; \\ 1, & \text{if } 2 \,||\, \rho. \end{cases}$$

If $Q = 1$ and ρ is even, then $U^e_{\rho+1}$ is replaceable by $(-1)^{mt-sn}$ in Theorem 88. Thus, our calculation of $(-1)^{x+y}$ is identical to the case $Q = -1$ and $4 \mid \rho$. □

Remark 37 For $U = F$, the case of an odd prime p of rank $\rho = p + 1$ (i.e., congruence (5.68)) is a subcase of "$4 \mid \rho$" in Theorem 92. Indeed, by Theorem 36, we must have $(Q \mid p) = -1$. Thus, since $Q = -1$, we have $p \equiv 3 \pmod 4$. Hence, $4 \mid p+1$. Note also that, by Lemma 15, $V_{p+1} \equiv 2Q \pmod p$. For these primes, we also recover (5.68) from (5.65).

When Theorem 92 is applicable, it provides a very effective way of computing a Lucasnomial modulo p. In fact, we get the following corollary which is very close to Lucas' theorem.

Corollary 93 Suppose $U(P, Q)$ is a fundamental Lucas sequence with $Q = \pm 1$ and p is an odd prime with even rank ρ. Assume m, n, and a are nonnegative integers with $a \geq 1$, $m = s_0 + s_1\rho + s_2 p\rho + \cdots + s_a p^{a-1}\rho$, and $n = t_0 + t_1\rho + t_2 p\rho + \cdots + t_a p^{a-1}\rho$, where $0 \leq s_0, t_0 < \rho$ and $0 \leq s_i, t_i < p$ for all $1 \leq i < a$. Then

$$\binom{m}{n}_U \equiv \prod_{i=1}^{a-1} \binom{s_i}{t_i} \cdot \binom{s_0}{t_0}_U \epsilon_{m,n} \pmod p,$$

where

$$\epsilon_{m,n} = \begin{cases} (-1)^{\lfloor m/\rho \rfloor t_0 - s_0 \lfloor n/\rho \rfloor} = (-1)^{t_0 \sum_{i\geq 1} s_i - s_0 \sum_{i \geq 1} t_i}, & \text{if } 4 \mid \rho \text{ or } Q = 1; \\ 1, & \text{if } 2 \,||\, \rho \text{ and } Q = -1. \end{cases}$$

Proof By Theorem 92, we obtain

$$\binom{m}{n}_U = \binom{\lfloor m/\rho \rfloor \rho + s_0}{\lfloor n/\rho \rfloor \rho + t_0}_U \equiv \binom{\lfloor m/\rho \rfloor}{\lfloor n/\rho \rfloor} \binom{s_0}{t_0}_U \epsilon_{m,n} \pmod p,$$

and the result follows by applying Lucas' theorem to the binomial coefficient $\binom{\lfloor m/\rho \rfloor}{\lfloor n/\rho \rfloor}$. □

Remark 38 The Lucasnomial triangle modulo p is easiest to construct when $Q = -1$ and $2 \,||\, \rho$. The initial triangle made of the first ρ lines, from 0 to $\rho - 1$, is repeated in the successive next blocks of ρ lines twice, three times, $\ldots, n$ times, where the kth copy in the nth block is multiplied by $\binom{n}{k} \pmod p$. Thus, once the initial triangle of ρ lines is built, the construction is similar and as convenient as for our ordinary Pascal triangle.

Example 94 (Of the use of Corollary 93 to compute some Lucasnomials modulo p)

1. If $U = F = U(1, -1)$, $p = 11$, then $\rho = 10$ and $2 \,||\, \rho$. Say $m = 252$ and $n = 131$. Then

$$252 = 2 \times 110 + 3 \times 10 + 1 \times 2,$$
$$131 = 1 \times 110 + 2 \times 10 + 1 \times 1.$$

Hence, the mixed-base digits (s_2, s_1, s_0) are $(2, 3, 2)$ and $(t_2, t_1, t_0) = (1, 2, 1)$. Thus, the Fibonomial modulo 11 is given by Corollary 93 as

$$\binom{252}{131}_F \equiv \binom{s_2}{t_2}\binom{s_1}{t_1}\binom{s_0}{t_0}_F = 2 \cdot 3 \cdot 1 = 6 \pmod{11}.$$

2. If $U = P = U(2, -1)$, the sequence of Pell numbers and $p = 3$, then $\rho = 4$.

Hence,

$$\binom{50}{13}_P \equiv \binom{1}{0}\binom{1}{1}\binom{2}{1}_P (-1)^{1\times(1+1)-2\times(1+0)} = 1 \cdot 1 \cdot 2 \cdot 1 = 2 \pmod{3},$$

since $\lfloor 50/4 \rfloor = 1 \cdot 9 + 1 \cdot 3$, $s_0 = 2$, $\lfloor 13/4 \rfloor = 1 \cdot 3$ and $t_0 = 1$. □

We end the section by giving a few related theorems from the literature.

Holte [39, Thm. 3] obtained the following curious, somewhat "Lucas-like" theorem, where $T = T(p)$ is the least period of U_n modulo p. This theorem also allows for the computing of a Lucasnomial modulo a prime.

Theorem 95 *Suppose $p \nmid Q$ is a prime, m and n are nonnegative integers, and λ is the maximum of 0 and $\lfloor r_T(m)/\rho \rfloor + \lfloor r_T(n)/\rho \rfloor - (p-1)$. Then*

$$\binom{m+n}{n}_U \equiv \binom{\lfloor m/\rho \rfloor + \lfloor n/\rho \rfloor}{\lfloor n/\rho \rfloor}\binom{\lfloor r_T(m)/\rho \rfloor + \lfloor r_T(n)/\rho \rfloor + \lambda M}{\lfloor r_T(n)/\rho \rfloor + \lambda M}^{-1} \times \binom{r_T(m) + r_T(n) + \lambda T}{r_T(n) + \lambda T}_U \pmod{p},$$

where $\rho = \rho(p)$, $T = T(p)$, $r_T(x)$ is the remainder in the division of x by T, and $M = T/\rho$ is the multiplier.

Remark 39 The multiplier $M = M(p)$ for the Fibonacci sequence can only be 1, 2 or 4 (with equal frequency, i.e., each value of M occurs for a set of primes whose natural density is 1/3 [6, Thm. 5.1]; see Chap. 9 for prime density questions). This allows for a simpler expression of Holte's theorem when $U = F$.

Corollary 96 Suppose $p \neq 5$ is a prime and m and n are nonnegative integers. Then

$$\binom{m+n}{n}_F \equiv \binom{\lfloor m/\rho \rfloor + \lfloor n/\rho \rfloor}{\lfloor n/\rho \rfloor}\binom{\lfloor r_T(m)/\rho \rfloor + \lfloor r_T(n)/\rho \rfloor}{\lfloor r_T(n)/\rho \rfloor}^{-1} \times \binom{r_T(m) + r_T(n)}{r_T(n)}_F \pmod{p},$$

where $\rho = \rho(p)$, $T = T(p)$, and $r_T(x)$ is the remainder in the division of x by T. Moreover, if $2 \,||\, \rho$, then

$$\binom{m+n}{n}_F \equiv \binom{\lfloor m/\rho \rfloor + \lfloor n/\rho \rfloor}{\lfloor n/\rho \rfloor} \binom{r_T(m) + r_T(n)}{r_T(n)}_F \pmod{p}. \tag{5.69}$$

Proof By [6, Thm. 5.1] or [78], for $p \neq 5$ a prime, we find that

$$\begin{aligned} M(p) = 1 &\iff 2 \,||\, \rho \text{ or } p = 2, \\ M(p) = 2 &\iff 4 \mid \rho, \\ M(p) = 4 &\iff \rho \text{ is odd and } p \neq 2. \end{aligned}$$

If $M = 1$, then $r_T(x) < T = \rho$ so that $\lambda = 0$. If $M = 2$, then $r_T(x) < T = 2\rho$. Hence, $\lfloor r_T(m)/\rho \rfloor + \lfloor r_T(n)/\rho \rfloor \leq 2$, and since $p - 1 \geq 2$, $\lambda = 0$ again. If $M = 4$, then $\lfloor r_T(m)/\rho \rfloor + \lfloor r_T(n)/\rho \rfloor \leq 3 + 3$. But the least prime $p \neq 5$ for which $M = 4$ is $p = 13$ of rank 7. Since $13 - 1 > 6$, we see that $\lambda = 0$ once more. If $2 \,||\, \rho$, then $r_T(x) = 0$ for all integers $x \geq 0$ so the middle term on the RHS of the corollary is $\binom{0}{0}^{-1}$. This explains (5.69). □

Example 97 For the sake of comparison, we apply Corollary 96 to the same Fibonomial $\binom{252}{131}_F$ and the same prime $p = 11$ as used in Example 94. Since

$$\binom{252}{131}_F = \binom{252}{121}_F = \binom{131+121}{121}_F,$$

let us put $m = 131$ and $n = 121$. Since $\rho_F(11) = 10$, we have $2 \,||\, \rho$, consequently, by the results in [6], $M = 1$. (Indeed, $F_{11} = 89 \equiv 1 \pmod{11}$.) Thus, $r_T(m) = r_T(n) = 1$. By (5.69) and Lucas' theorem, we get

$$\begin{aligned} \binom{131+121}{121}_F &\equiv \binom{13+12}{12}\binom{2}{1}_F = \binom{2 \cdot 11 + 3}{1 \cdot 11 + 1} \cdot 1 \\ &\equiv \binom{2}{1}\binom{3}{1} = 2 \times 3 = 6 \pmod{11}, \end{aligned}$$

in agreement with our previous calculation. □

In 2002, Hu [40] published a result similar to Theorem 88, but for generalized binomial coefficients with respect to companion Lucas sequences V, namely,

Theorem 98 *Suppose $U(P, Q)$ is a regular and nondegenerate Lucas sequence. If q is a positive integer, then*

$$\binom{m/2}{n/2}\binom{mq+s}{nq+t}_V \equiv \binom{m}{n}\binom{s}{t}_V (-Q^q)^f \pmod{V_q^*}, \tag{5.70}$$

where m, n, s, and t are nonnegative integers, m and n are even, s and t are less than q, f is $(nq+t)(m-n)/2+n(s-t)/2$, and V_q^* is the largest factor of V_q prime to $V_0V_1\cdots V_{q-1}$.

5.8 Wolstenholme's Congruence

In 1862, Wolstenholme [84] made a remarkable discovery: if $p \geq 5$ is a prime number, then the binomial coefficient $\binom{2p-1}{p-1}$ is congruent to 1 modulo the cube of p. That is,

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}. \tag{5.71}$$

It had been observed by Babbage [4] in 1819 that congruence (5.71) held modulo p^2 for $p \geq 3$ since

$$\binom{2p}{p} = \sum_{k=0}^{p} \binom{p}{k}\binom{p}{p-k} = \sum_{k=0}^{p} \binom{p}{k}^2 \equiv \binom{p}{0} + \binom{p}{p} = 2 \pmod{p^2}.$$

Hence, dividing each side of the above congruence by 2 yields that $\binom{2p-1}{p-1} \equiv 1 \pmod{p^2}$. Wolstenholme, in finding (5.71), got the intermediary interesting congruence for the harmonic number H_{p-1}, also valid for $p \geq 5$:

$$H_{p-1} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p^2}. \tag{5.72}$$

(In [42, p. 93], the authors mentioned a remark of Rao who pointed out that congruence (5.72) and some of its extensions had been anticipated by Waring in 1782. Thus, Babbage could have discovered Wolstenholme's improved congruence.)

Deriving (5.71) from (5.72) only requires a few steps. Indeed,

$$\begin{aligned}\binom{2p-1}{p-1} &= \frac{1}{(p-1)!}\prod_{i=1}^{p-1}(p+i) \\ &\equiv 1 + pH_{p-1} + p^2 \sum_{0<i<j<p} \frac{1}{ij} \\ &\equiv 1 + p^2 \sum_{0<i<j<p} \frac{1}{ij} \pmod{p^3}.\end{aligned} \tag{5.73}$$

This yields (5.71) provided we verify that $\sum_{0<i<j<p} \frac{1}{ij}$ is $0 \pmod{p}$. But

$$H_{p-1}^2 = \sum_{0<i<p} \frac{1}{i^2} + 2 \sum_{0<i<j<p} \frac{1}{ij},$$

and since $p \geq 5$, we have

$$\sum_{0<i<p} \frac{1}{i^2} \equiv \sum_{0<i<p} i^2 = \frac{(p-1)p(2p-1)}{6} \equiv 0 \pmod{p}.$$

Therefore, we do have $\sum_{0<i<j<p} \frac{1}{ij} \equiv 0 \pmod{p}$.

Prior to writing a survey on Lucas' theorem, i.e., on Theorem 87, Meštrović had written yet another large survey on Wolstenholme's theorem and its various generalizations, this time up until 2012 [62]. However, Meštrović's survey, although it included a final section on q-analogues of Wolstenholme's congruence, did not include the research aimed at finding a generalization of the Wolstenholme congruence with respect to Lucasnomials. This is chiefly the story we recount in the present section.

To describe this research, we need to mention two early generalizations of Wolstenholme's congruence, namely, the *Wolstenholme-Glaisher congruence* [31, 32] of 1900, which asserts that for all integers $k \geq 0$,

$$\binom{(k+1)p-1}{p-1} \equiv 1 \pmod{p^3}, \tag{5.74}$$

and the further 1952 generalization of Brun et al. [21] which states that

$$\binom{mp}{np} \equiv \binom{m}{n} \pmod{p^3}, \tag{5.75}$$

for all nonnegative integers m and n and all primes $p \geq 5$.

Remark 40 Multiplying both sides of (5.74) by $k+1$, one obtains (5.75) with $m = k+1$ and $n = 1$. Clearly, (5.75) supersedes the Wolstenholme-Glaisher and the Wolstenholme congruences. However, in some sense, the Wolstenholme congruence is the inner core of (5.75): Bailey [5] re-proves the Wolstenholme congruence and uses it as a basis to obtain (5.74) and (5.75) by two successive inductive proofs. Similarly, this time by a combinatorial argument, Stanley [75, Sol. of exercise 1.14, p. 165] reduces the proof of (5.75) to the Wolstenholme congruence $\binom{2p}{p} \equiv 2 \pmod{p^3}$.

Kimball and Webb sought some analogues and generalizations of these various theorems with respect to Fibonomials and Lucasnomials in a series of papers in the 1990s [47–50], starting the investigation, as often, with Fibonacci numbers. It is curious to observe that parallel and independent researches on q-analogues of all these same theorems were simultaneously carried out in the 1990s and refined further in later years. We refer the reader to Meštrović's [62, Sect. 11] and only mention, for the sake of comparison with Lucasnomial results, the 1999 polynomial congruence of Andrews [2, Thm. 3]

$$\binom{mp}{np}_q \equiv \binom{m}{n}_{q^p} q^{n(m-n)p(p-1)/2} \pmod{\Phi_p(q)^2}, \tag{5.76}$$

where $p \geq 3$ is a prime, $\binom{m}{n}_{q^p}$ is obtained by replacing every appearance of q by q^p in $\binom{m}{n}_q$, m and n are nonnegative integers, and $\Phi_p(q) = 1 + q + q^2 + \cdots + q^{p-1}$ is the pth cyclotomic polynomial in q. By letting q tend to 1, we see that congruence (5.76) is a weak generalization of the Brun et al. congruence, since we only get the congruence modulo p^2.

Kimball and Webb started [47] by proving a p^2-analogue of (5.75) for the Fibonacci sequence. Suppose $p \geq 3$ is a prime number and ρ is the rank of p in the Fibonacci sequence $F = U(1, -1)$. They find that

$$\binom{m\rho}{n\rho}_F \equiv \epsilon^{(m-n)n\rho} \binom{m}{n} \pmod{p^2}, \tag{5.77}$$

where

$$\epsilon = \begin{cases} 1, & \text{if } 2 \,||\, \rho; \\ -1, & \text{if } 4 \mid \rho; \\ \sqrt{-1} \pmod{p^2}, & \text{if } \rho \text{ is odd,} \end{cases}$$

and $m \geq n \geq 0$ are integers. (Note that when $(m-n)n\rho$ is odd, the theorem does not say which of the two square roots of $-1 \pmod{p^2}$ to select. For instance, if $p = 5$, then the theorem holds with $\epsilon = -7$, not 7. From (5.82), we will see that $\epsilon \equiv L_\rho/2 \pmod{p^2}$. Note further that if ρ is odd, putting $U = F$, $V = L$, and $n = \rho$ in (2.8) yields that $L_\rho^2/4 \equiv -1 \pmod{p^2}$.) Another remark: if ρ is even, then Theorem 92, which is a congruence that yields $\binom{m\rho}{n\rho}_F \pmod{p}$, remains valid modulo p^2 by (5.77).

Our two pioneers,† Kimball and Webb, in their next paper [48], described some analogues of the congruence of Wolstenholme for the harmonic number H_{p-1} (5.72), for the Wolstenholme-Glaisher congruence, and, under conditions on the rank of p, for the congruence of Brun et al. modulo p^3, all in the Fibonacci context: Let F and L designate, as usual, the sequences of Fibonacci and Lucas numbers. If $p \geq 7$ is a prime and its rank ρ in F is $p-1$ or $p+1$, then

$$\sum_{0<i<\rho} \frac{L_i}{F_i} \equiv 0 \pmod{p^2}. \tag{5.78}$$

(It is an analogue of (5.72) as we may state (5.72) in the equivalent form $\sum_{0<i<p} 2/i \equiv 0 \pmod{p^2}$, since for $(P, Q) = (2, 1)$, we have $U_i = i$ and $V_i = 2$ for all i.)

Much in the way we deduced Wolstenholme's congruence (5.71) from Wolstenholme's divisibility of the harmonic number H_{p-1} by p^2, Kimball and Webb obtain a Fibonacci analogue of the Wolstenholme-Glaisher congruence (5.74). Suppose $p \geq 7$ is a prime number of rank $\rho = p - \epsilon_p$, where

† The term "pioneer" is meant as a true compliment; too often credit only rests on those who put the final dot.

$$\epsilon_p = (5\,|\,p) = (p\,|\,5) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod 5; \\ -1, & \text{if } p \equiv \pm 2 \pmod 5. \end{cases}$$

Then

$$\binom{(k+1)\rho - 1}{\rho - 1}_F \equiv \epsilon_p^k \pmod{p^3}. \tag{5.79}$$

Finally, they found that under the same rank condition on p, i.e., $\rho = p - \epsilon_p$ and $\epsilon_p = \pm 1$, we have for all $p \geq 7$, all integers $m \geq n \geq 0$,

$$\binom{m\rho}{n\rho}_F \equiv \epsilon_p^{(m-n)n} \binom{m}{n}_{F'} \pmod{p^3}, \tag{5.80}$$

where $F' = U(L_\rho, (-1)^\rho) = U(L_\rho, 1)$.

They also pointed out a corollary of (5.80), i.e.,

$$\binom{mT}{nT}_F \equiv \begin{cases} \binom{m}{n}_{F'}, & \text{if } \rho = p - 1; \\ \binom{2m}{2n}_{F'}, & \text{if } \rho = p + 1; \end{cases} \pmod{p^3}, \tag{5.81}$$

where $T = T(p)$ is the least period of F modulo p.

We remark here that if $U = U(2, 1)$, Lucasnomials with respect to U are the usual binomial coefficients. In this case, $\rho_U(p) = p = T(p)$. Therefore, it makes sense to look for analogues where either ρ or T replaces p in the binomial coefficient $\binom{mp}{np}$ of (5.75).

In [49], Kimball and Webb obtained a generalization of (5.77) for general Lucasnomials. Suppose $U(P, Q)$ is a regular nondegenerate Lucas sequence and $p \geq 3$ is a prime of rank ρ in U. Then, for all integers $m \geq n \geq 0$,

$$\binom{m\rho}{n\rho}_U \equiv \binom{m}{n} (V_\rho/2)^{(m-n)n\rho} \pmod{p^2}, \tag{5.82}$$

where V is the companion Lucas sequence of $U(P, Q)$.

We note in passing that if we put $s = t = 0$ in (5.65), then we obtain precisely the above congruence albeit modulo p, rather than p^2, since, by Theorem 88, $e = n(m - n)\rho$.

From (5.82), they derive several congruences to express $\binom{mT}{nT}_U$ modulo p^2, where again T is the minimal period of U modulo p. The case $Q = \pm 1$ is particularly simple since

$$\binom{mT}{nT}_U \equiv \binom{mM}{nM} \pmod{p^2},$$

where M is the multiplier defined in Theorem 95 as the integer T/ρ.

In their final paper on this theme [50], they essentially generalized the results they had obtained in [48] in the Fibonacci context to general Lucasnomials in the form of the next theorem.

Theorem 99 *Suppose $U = U(P,Q)$ is a nondegenerate fundamental Lucas sequence and $p \geq 5$, $p \nmid Q$, is a prime number of rank ρ. Define S as $\sum_{0<n<\rho} \frac{V_n}{U_n}$. Then*

$$\begin{aligned}
&\textbf{1.} \quad S \equiv 0 \pmod{p},\\
&\textbf{2.} \quad D = 0 \implies S \equiv 0 \pmod{p^2},\\
&\textbf{3.} \quad D \neq 0 \text{ and } \rho = p \pm 1 \implies S \equiv 0 \pmod{p^2},
\end{aligned}$$

where as usual D denotes the discriminant $P^2 - 4Q$.

For some reason, they did not fully complete the investigation. For one would naturally want to know whether extensions of the $\pmod{p^3}$- congruences (5.79) and (5.80) which hold for the Fibonacci sequence exist in a more general form for Lucasnomials.

This was in large part done by Shi [73] in 2007. She (Shi) obtained the following theorem as a generalization of (5.80) and of the Brun et al. congruence (5.75).

Theorem 100 *Let $U(P,Q)$ be a regular nondegenerate fundamental Lucas sequence. Let $p \geq 5$, $p \nmid Q$, be a prime number. Suppose the rank of appearance ρ of p in U is $p-1$ or $p+1$. Then, for all nonnegative integers m and n,*

$$\binom{m\rho}{n\rho}_U \equiv (-1)^{(m-n)n} Q^{(m-n)n\binom{\rho}{2}} \binom{m}{n}_{U'} \pmod{p^3},$$

where $U' = U(V_\rho, Q^\rho)$.

Shi also has a theorem, [73, Thm. 2], that expresses in an elaborate way Lucasnomials $\binom{m\rho+s}{n\rho+t}_U$ modulo p^2, with no restrictive hypotheses on ρ, the rank of p.

In 2015, Ballot, unaware at the time of Shi's contribution (of this he is aware!), obtained a theorem [10, Thm. 13] identical to Theorem 100 but with broader hypotheses: The theorem holds modulo p^3 ($p \geq 5$) without the restriction that U be regular and for all primes of *maximal* rank, i.e., of rank $p - \epsilon_p$, where $\epsilon_p = (D \,|\, p)$ is allowed to be zero. Moreover, the theorem holds modulo p^2 ($p \geq 3$), instead of p^3, if no restrictive hypothesis is placed on the rank ρ. Thus, with $p \geq 5$, $\rho = \rho_U(p)$ maximal, and $U' = U(V_\rho, Q^\rho)$, we find that

$$\binom{m\rho}{n\rho}_U \equiv \big(-Q^{\rho/2}\big)^{(\rho-1)n(m-n)} \binom{m}{n}_{U'} \pmod{p^3}. \tag{5.83}$$

Incidentally, the generalized Wolstenholme-Glaisher theorem [10, Thms. 3 and 7] for general Lucasnomials $\binom{*}{*}_{U(P,Q)}$ has the shape

$$\binom{(k+1)\rho - 1}{\rho - 1}_U \equiv (-1)^{k(\rho-1)} Q^{k\rho(\rho-1)} \pmod{p^a}, \tag{5.84}$$

where $p \geq 3$, $p \nmid Q$, is a prime number, $k \geq 0$ is an integer, and

$$a = 2 + [\, p \geq 5 \,] \cdot [\, \rho \text{ is maximal }].$$

We observe that (5.83) is a generalization of Brun's congruence (5.75), but Theorem 100 is not. Indeed, if $U = U(2,1)$, then, for all $n \geq 0$, $U_n = n$ and $V_n = 2$. In particular, $U' = U$. Since $\rho_U(p) = p$ is maximal with $\epsilon_p = 0$, (5.83) applies. Because $Q = 1$ and $\rho - 1$ is even for all primes $p \geq 5$, the RHS of (5.83) is 1, and we recover Brun's congruence (5.75).

More refined congruences than Wolstenholme's for binomial coefficients $\binom{2p-1}{p-1}$ (or for the Wolstenholme-Glaisher congruence) have been the object of many papers. Meštrović [62, pp. 4–7] has compiled a number of congruences for $\binom{2p-1}{p-1}$ modulo p^x, where x varies between 4 and 9. These formulas involve powers of p with coefficients which typically are expressed in terms of generalized harmonic sums and/or Bernoulli numbers. The interested reader may wish to consult two more recent papers of interest in this regard [55, 70], which gave methods for obtaining higher power congruences for $\binom{2p-1}{p-1}$.

Ballot [10, p. 12] chose three congruences that expressed $\binom{2p-1}{p-1}$ modulo p^5 as well as the (mod p^6)-congruence of Tauraso [77]

$$\binom{2p-1}{p-1} \equiv 1 + 2p \sum_{0<i<p} \frac{1}{i} + \frac{2p^3}{3} \sum_{0<i<p} \frac{1}{i^3} \pmod{p^6},$$

all valid for $p \geq 7$, to examine their potential Lucasnomial generalizations. For instance, Tauraso's congruence generalizes [10, Thm. 28] as

$$\binom{2\rho-1}{\rho-1}_U \equiv (-1)^{\rho-1} Q^{\frac{\rho(\rho-1)}{2}} \left(1 + 2\frac{U_\rho}{V_\rho} \sum_{0<t<p} \frac{V_t}{U_t} + \frac{2}{3}\frac{U_\rho^3}{V_\rho^3} \sum_{0<t<p} \frac{V_t^3}{U_t^3}\right) \pmod{p^6},$$

where $p \geq 7$ is a prime of maximal rank ρ with respect to a general Lucas sequence $U(P,Q)$.

In 2013, Ohtsuka [64] proposed in the "Advanced Problems and Solutions" of the Fibonacci Quarterly (openly available online) to prove that the congruence

$$\binom{(k+1)p-1}{p-1}_F \equiv (-1)^{k(p-1)/2} \pmod{F_p^2 L_p}$$

holds for all primes $p \geq 3$ and all integers $k \geq 0$, where F_p and L_p are the pth Fibonacci and Lucas numbers. Since the congruence is obviously an analogue of the Wolstenholme-Glaisher for Fibonomials, this spurred Ballot to find a general Lucasnomial analogue in this direction. Thus, if (U,V) is a pair of Lucas sequences with parameters P and Q and $p \geq 3$ is a prime, then, for all $k \geq 0$, we have [14, Thm. 3]

$$\binom{(k+1)p-1}{p-1}_U \equiv Q^{kp(p-1)/2} \pmod{U_p^2 V_p / P}. \tag{5.85}$$

There is a corresponding Lucasnomial generalization [14, Thm. 17] of congruence (5.75) of Brun et al., namely, for $p \geq 3$, m and n nonnegative integers,

$$\binom{mp}{np}_U \equiv Q^{n(m-n)p(p-1)/2} \binom{m}{n}_{U'} \pmod{U_p^a V_p/P}, \tag{5.86}$$

where $U' = U(V_p, Q^p)$ and $a = 2 + [\,p \geq 5\,] \cdot [\,U_p = \pm p\,]$.

The factor U_p^2 of the above modulus $U_p^a V_p/P$ in (5.86) suggests looking for a possible upgrading of the modulus of the q-congruence of Andrews (5.76). Indeed, U_p plays the role of the polynomial $\Phi_p(q)$.

Point **3** of Theorem 99 is not quite a generalization of the Wolstenholme congruence (5.72) for H_{p-1}, because the authors did not address the case $\epsilon_p = 0$ (only the case $D = 0$). This is at least an analogue of (5.72). A true generalization came years later. In 2008, in a too-rare link established between the q-theory and the Lucas theory, Pan [66] used a q-analogue of (5.72), expressing $\sum_{i=1}^{m-1} \frac{1}{i_q}$ modulo $\Phi_m(q)^2$, to go further and establish that

$$\sum_{i=1}^{m-1} \frac{V_i}{U_i} \equiv \frac{(m^2-1)D}{6} \cdot \frac{U_m}{V_m} \pmod{P_m^2}, \tag{5.87}$$

where $m \geq 5$ is an integer, (U, V) is a pair of Lucas sequences with parameters P and Q, $D = P^2 - 4Q$, and, as in Hu and Sun's Theorem 88, P_m is the largest factor of U_m relatively prime to $U_2 U_3 \cdots U_{m-1}$. Note that if $\rho = m \geq 5$ and $\rho = p - \epsilon_p$ is the rank of a prime p, then $p \geq \rho - 1 \geq 4$ so $p \geq 5$, and, in all three cases of $\epsilon_p = (D \,|\, p) \in \{0, \pm 1\}$, the factor $(m^2-1)DU_m$ is zero modulo p^2 so that for all primes $p \geq 5$ of maximal rank, we find that

$$\sum_{0<n<\rho} \frac{V_n}{U_n} \equiv 0 \pmod{p^2}. \tag{5.88}$$

Thus, Pan's result implies (5.72) since (5.88) is a true generalization of (5.72). In [8, Chap. 4], it was observed that, for some values of D, there are other pairs (X, Y) of second-order recurring sequences with characteristic polynomial $x^2 - Px + Q$, for which sums of ratios $\sum_i (X_i/Y_i)$, where the sum is over intervals of length ρ on which $Y \not\equiv 0 \pmod{p}$, are zero modulo p^2, if $\rho = \rho_U(p)$ is maximal. In fact, it was noticed that for all pairs (X, Y) studied in [8] for which the Wolstenholme phenomenon occurred, X and Y differed by V with respect to the Laxton group law. Ward [81] defined and Laxton later used the following terminology: Two second-order linear recurrences with the same characteristic polynomial are said to be *polar* if they differ by V in that group. (The polarity relation is symmetric.) It is not true that the Wolstenholme congruence holds for all polar pairs of sequences. Thus, it would be of interest to describe exactly when the phenomenon takes place. (The Laxton group will be described in Chap. 9, Sect. 9.7.)

Leudesdorf [54] proved in 1889, the year of the completion of the Eiffel Tower in Paris, that if $\ell \geq 1$ is an odd integer and $p \geq \ell + 4$ is a prime number, then

$$\sum_{0<n<p} \frac{1}{n^\ell} \equiv 0 \pmod{p^2}. \tag{5.89}$$

This is an extension of Wolstenholme's congruence (5.72) since for $\ell = 1$, (5.89) says that for all primes $p \geq 5$, $H_{p-1} \equiv 0 \pmod{p^2}$. Congruence (5.89) also appears as Theorem 131 in the classic book of Hardy and Wright [42]. A generalization of (5.89) to Lucasnomials was found in 2014 by Ballot [9, Thm. 3]. Suppose (U, V) is a pair of Lucas sequences with parameters P and Q. If $\ell \geq 1$ is an odd integer and $p \geq \ell + 4$, $p \nmid Q$, is a prime of maximal rank $\rho = p - \epsilon_p$, $\epsilon_p = (D \,|\, p)$, in U, then

$$\sum_{0<n<\rho} \frac{V_n^\ell}{U_n^\ell} \equiv 0 \pmod{p^2}. \tag{5.90}$$

In closing this section, we note that Wolstenholme's congruence for H_{p-1} (5.72) says that the sum of all Egyptian fractions $1/i$, for $1 \leq i \leq p$ (i prime to p), is zero modulo p^2. Leudesdorf [54] also found an extension of (5.72) to all composite integers $m \geq 1$, not just for m prime. That is,

Theorem 101 *Let m be an integer ≥ 1. Then*

$$\sum_{\substack{i=1 \\ \gcd(i,m)=1}}^{m} \frac{1}{i} \equiv 0 \pmod{m^2/e_m},$$

where $e_m = \gcd(m, 6)$, unless $m = 2^a$, $a \geq 1$, when $e_m = 4$.

Some work related to generalizations of Theorem 101 for Lucasnomials can be found in the papers [7, 43]; see in particular [7, Thm. 3].

5.9 A Word on Lehmernomials

We define here *Lehmernomials*, or *Lehmernomial coefficients*,

$$\binom{m}{n}_{\bar{U}},$$

as generalized binomial coefficients with respect to a Lehmer sequence $\bar{U}(R, Q)$; see Sect. 4.4 for the definition of the Lehmer sequences $\bar{U}(R, Q)$ and $\bar{V}(R, Q)$ and a few of their basic properties.

Much of the theory developed with respect to Lucasnomials in this chapter may have a potential comparable theory for Lehmernomials. Here, we merely

define them and observe that they are integers and that Lehmernomial Catalan numbers and Lehmernomial Fuss-Catalan numbers are also integers.

Definition 8 (Lehmernomial Fuss-Catalan numbers) Let $a \geq 2$ and n be integers and $\bar{U}(R,Q)$ be a U-Lehmer sequence. The numbers

$$\frac{1}{\bar{U}_{(a-1)n+1}}\binom{an}{n}_{\bar{U}}$$

are called Lehmernomial Catalan numbers if $a = 2$ and Lehmernomial Fuss-Catalan numbers if $a \geq 3$ (with respect to $\bar{U}(R,Q)$).

Theorem 102 *Lehmernomials are integers.*

Proof By (2.42), we get

$$U_m(\sqrt{R},Q) = U_{n+1}(\sqrt{R},Q)U_{m-n}(\sqrt{R},Q) - QU_n(\sqrt{R},Q)U_{m-n-1}(\sqrt{R},Q).$$

Suppose m and n are even integers. Then dividing both sides of the above equation by $\sqrt{R}$, we obtain

$$\begin{aligned}\bar{U}_m(R,Q) &= U_{n+1}(\sqrt{R},Q)\cdot\frac{U_{m-n}(\sqrt{R},Q)}{\sqrt{R}} - Q\frac{U_n(\sqrt{R},Q)}{\sqrt{R}}\cdot U_{m-n-1}(\sqrt{R},Q)\\ &= \bar{U}_{n+1}(R,Q)\cdot\bar{U}_{m-n}(R,Q) - Q\bar{U}_n(R,Q)\bar{U}_{m-n-1}(R,Q).\end{aligned}$$

For all parity cases of m and n, we obtain similarly

$$\bar{U}_m = R_{m,n}\bar{U}_{n+1}\bar{U}_{m-n} - Q_{m,n}\bar{U}_n\bar{U}_{m-n-1}, \tag{5.91}$$

where

$$R_{m,n} = \begin{cases}1, & \text{if } mn \text{ is even;}\\ R, & \text{if } mn \text{ is odd;}\end{cases} \quad \text{and} \quad Q_{m,n} = \begin{cases}RQ, & \text{if } m \text{ is odd and } n \text{ even;}\\ Q, & \text{otherwise.}\end{cases}$$

Using Lemma 31, we find that

$$\binom{m}{n}_{\bar{U}} = R_{m,n}\bar{U}_{n+1}\binom{m-1}{n}_{\bar{U}} - Q_{m,n}\bar{U}_{m-n-1}\binom{m-1}{n-1}_{\bar{U}}. \tag{5.92}$$

Using (5.92), the integrality of Lehmernomials follows by carrying an induction on m. □

Theorem 103 *Lehmernomial Catalan numbers satisfy*

$$\frac{1}{\bar{U}_{n+1}}\binom{2n}{n}_{\bar{U}} = \binom{2n-1}{n}_{\bar{U}} - Q\binom{2n-1}{n-2}_{\bar{U}}$$

and, consequently, are integers.

Proof Note that $R_{2n,n} = 1$ and $Q_{2n,n} = Q$. The same technique used to obtain (5.47) yields the result. □

More generally, we have the following:

Theorem 104 *Lehmernomial Fuss-Catalan numbers satisfy*

$$\frac{1}{\bar{U}_{(a-1)n+1}}\binom{an}{n}_{\bar{U}} = \binom{an-1}{n}_{\bar{U}} - Q_{an,(a-1)n}\frac{\bar{U}_{(a-1)n}}{\bar{U}_n}\binom{an-1}{n-2}_{\bar{U}}$$

and, consequently, are integers.

Proof Replace m by an and n by $(a-1)n$ in (5.92), note that $R_{an,(a-1)n} = 1$, divide through by $\bar{U}_{(a-1)n+1}$, and rearrange the last term on the RHS of the identity as done in [13, Lemma 5]. Integrality follows from the integrality of Lehmernomials and the fact that $\bar{U}(R, Q)$ is a divisible sequence. □

References

1. M. Abouzaid, *Les nombres de Lucas et Lehmer sans diviseur primitif*, (French) [Lucas and Lehmer numbers with no primitive divisors], J. Théor. Nombres Bordeaux **18** (2006), 299–313.
2. G. Andrews, *q-analogues of the binomial coefficient congruences of Babbage, Wolstenholme and Glaisher*, Discrete Math. **204** (1999), 15–25.
3. J. Azose and A. Benjamin, *A tiling interpretation of the q-binomial coefficients*, Fibonacci Quart. **58** (2020), no. 2, 99–125.
4. C. Babbage, *Demonstration of a theorem relating to prime numbers*, Edinburgh Philosophical J. **1** (1819), 46–49.
5. D. F. Bailey, *Two p^3 variations of Lucas' theorem*, J. Number Theory **35** (1990), 208–215.
6. C. Ballot and M. Elia, *Rank and period of primes in the Fibonacci sequence. A trichotomy*, Fibonacci Quart. **45** (2007), no. 1, 56–63.
7. C. Ballot, *A further generalization of a congruence of Wolstenholme*, J. Integer Seq. **15** (2012), Article 12.8.6.
8. C. Ballot, *Lucas sequences with cyclotomic root field*, Dissertationes Math. **490** (2013), 92 pp.
9. C. Ballot, *On a congruence of Kimball and Webb involving Lucas sequences*, J. Integer Seq. **17** (2014), Article 14.1.3.
10. C. Ballot, *The congruence of Wolstenholme for generalized binomial coefficients related to Lucas sequences*, J. of Integer Seq. **18** (2015) Article 15.5.4.
11. C. Ballot, *Divisibility of Fibonomials and Lucasnomials via a general Kummer rule*, Fibonacci Quart. **53** (2015), 194–205.
12. C. Ballot, *Divisibility of the middle Lucasnomial coefficient*, Fibonacci Quart. **55** (2017), 297–308.

13. C. Ballot, *Lucasnomial Fuss-Catalan numbers and related divisibility questions*, J. Integer Seq. **21** (2018), Article 18.6.5.
14. C. Ballot, *Another Lucasnomial generalization of Wolstenholme's congruence*, J. Integer Seq. **23** (2020), Article 20.3.7.
15. C. Ballot, *The p-adic valuation of Lucasnomials when p is a special prime*, J. Integer Seq. **24** (2021), Article 21.1.4.
16. A. Benjamin and J. Quinn, *Proofs That Really Count: The Art of Combinatorial Proof*, The Dolciani Mathematical Expositions **27**, Mathematical Association of America, Washington, DC, 2003.
17. A. Benjamin and S. Plott, *A combinatorial approach to fibonomial coefficients*, Fibonacci Quart. **46-47** (2008/2009), 7–9, 276.
18. A. Benjamin and E. Reiland, *Combinatorial proofs of Fibonomial identities*, Fibonacci Quart. **52** (2014), no. 5, 28–34.
19. C. Bennett, J. Carrillo, J. Machacek and B. Sagan, *Combinatorial interpretations of Lucas analogues of binomial coefficients and Catalan numbers*, Ann. Comb. **24** (2020), no. 3, 503–530.
20. Y. Bilu, G. Hanrot, P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, With an appendix by M. Mignotte, J. Reine Angew. Math. **539** (2001), 75–122.
21. V. Brun, J. O. Stubban, J. E. Fjeldstad, R. Tambs Lyche, K. E. Aubert, W. Ljunggren, E. Jacobsthal, *On the divisibility of the difference between two binomial coefficients*. Den 11te Skandinaviske Matematikerkongress, Trondheim, 1949, 42–54. Johan Grundt Tanums Forlag, Oslo, 1952.
22. L. Carlitz, *The characteristic polynomial of a certain matrix of binomial coefficients*, Fibonacci Quart. **3** (1965), 81–89.
23. X. Chen and B. Sagan, *The fractal nature of the Fibonomial triangle*, Integers **14** (2014), Paper No. A3.
24. M. Debellevue and E. Kryuchkova, *Fractal behavior of the Fibonomial triangle modulo a prime p, where the rank of apparition of p is* $p + 1$, Fibonacci Quart. **56** (2018), no. 2, 113–120.
25. S. Ekhad, *The Sagan-Savage Lucas-Catalan polynomials have positive coefficients*, (2011), available at https://arxiv.org/abs/1101.4060
26. N. J. Fine, *Binomial Coefficients Modulo a Prime*, Amer. Math. Monthly **54** (1947), 589–592.
27. R. D. Fray, *Congruence properties of ordinary and q-binomial coefficients*, Duke Math. J. **34** (1967), 467–480.
28. G. Fontené, *Généralisation d'une formule connue*, Nouv. Ann. Math., (4) **15** (1915), 112.
29. G. Freitas, J. Lopes and D. Marques, *On congruences involving some Fibonomial coefficients*, Integers **19** (2019), Paper No. A13.
30. J. Fürlinger and J. Hofbauer, *q-Catalan numbers*, J. Combin. Theory Ser. A 40 (1985), 248–264.
31. J. W. L. Glaisher, *Congruences relating to the sums of products of the first n numbers and to other sums of products*, Quart. J. Math. **31** (1900), 1–35.

32. J. W. L. Glaisher, *On the residues of the sums of products of the first $p-1$ numbers, and their powers, to modulus p^2 or p^3*, Quart. J. Math. **31** (1900), 321–353.
33. R. Graham, D. Knuth and O. Patashnik, *Concrete Mathematics*, Second Edition, Addison-Wesley Publishing Company, 1989, (June 2013 Printing).
34. H. W. Gould, *The bracket function and Fontené-Ward generalized binomial coefficients with application to Fibonomial coefficients*, Fibonacci Quart. **7** (1969), 23–40, 55.
35. H. W. Gould, *Fibonomial Catalan numbers: arithmetic properties and a table of the first fifty numbers*, Abstract 71T-A216, Notices Amer. Math. Soc. (1971), 938.
36. H. W. Gould, *A new primality criterion of Mann and Shanks and its relation to a theorem of Hermite with extension to Fibonomials*, Fibonacci Quart. **10** (1972) 355–364, 372.
37. V. E. Hoggatt, Jr., *Fibonacci numbers and generalized binomial coefficients*, Fibonacci Quart. **5** (1967), 383–400.
38. J. M. Holte, *A Lucas type theorem for Fibonomial-coefficient residues*, Fibonacci Quart. **32** (1994), 60–68.
39. J. M. Holte, *Residues of generalized binomial coefficients modulo a prime*, Fibonacci Quart. **38** (2000), 227–238.
40. H. Hu, *On Lucas ν-triangles*, Fibonacci Quart. **40** (2002), no. 4, 290–294.
41. H. Hu and Z.-W. Sun, *An extension of Lucas' theorem*, Proc. Amer. Math. Soc. **129** (2001), 3471–3478.
42. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford at the Clarendon Press, London, 4th edition, 1960.
43. E. Ieronymou, *Congruences involving sums of ratios of Lucas sequences*, J. Integer Seq. **17** (2014), Article 14.8.8.
44. D. Jarden, *Recurring Sequences*, Published by Riveon Lematimatika, Jerusalem (Israel), 1958, 42–45; second edition, 1966, 30–33.
45. D. Jarden and T. Motzkin, *The product of sequences with a common recursion of order* 2, Riveon Lematimatika **3** (1949), 25–27, 38 (Hebrew with English summary).
46. K. Killpatrick and J. Weaver, *A bijection for the Fibonomial coefficients*, Fibonacci Quart. **59** (2021), 14–18.
47. W. Kimball and W. Webb, *Congruence properties of Fibonacci numbers and Fibonacci coefficients modulo p^2*, Applications of Fibonacci Numbers **5**, Kluwer Acad. Publ., 1993, 399–403.
48. W. Kimball and W. Webb, *A congruence for fibonomial coefficients modulo p^3*, Fibonacci Quart. **33** (1995), 290–297.
49. W. Kimball and W. Webb, *Some congruences for generalized binomial coefficients*, Rocky Mountain J. Math. **25** (1995), 1079–1085.
50. W. Kimball and W. Webb, *Some generalizations of Wolstenholme's theorem*, Applications of Fibonacci Numbers **8** Kluwer Acad. Publ., 1999, 213–218.

51. J. Konvalina, *A unified interpretation of the binomial coefficients, the Stirling numbers, and the Gaussian coefficients*, Amer. Math. Monthly **107** (2000), no. 10, 901–910.
52. D. Knuth and H. Wilf, *The power of a prime that divides a generalized binomial coefficient*, J. Reine Angew. Math. **396** (1989), 212–219.
53. E. Kummer, *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, J. Reine Angew. Math. **44** (1852), 93–146.
54. C. Leudesdorf, *Some results in the elementary theory of numbers*, Proc. London Math. Soc. **20** (1889), 199–212.
55. P. Lombaers, *Generalizations of Wolstenholme's theorem via the p-adic logarithm*, Integers **20** (2020), Paper No. A42, 15 pp.
56. É. Lucas, *Théorie des fonctions simplement périodiques*, Amer. J. Math. **1** (1878), 184–240, 289–321.
57. P. MacMahon, *Combinatory Analysis*, 2 vol., Cambridge univ. Press, London, 1915-1916. Reprinted, Chelsea, New York, 1960.
58. D. Marques and P. Trojovský, *On parity of Fibonomial numbers*, Util. Math. **97** (2015), 129–135.
59. D. Marques and P. Trojovský, *On divisibility of Fibonomial coefficients by* 3, J. Integer Seq. **15** (2012), Article 12.6.4.
60. D. Marques and P. Trojovský, *The p-adic order of some fibonomial coefficients*, J. Integer Seq. **18** (2015), Article 15.3.1.
61. D. Marques, J. Sellers and P. Trojovský, *On divisibility properties of certain Fibonomial coefficients by a prime*, Fibonacci Quart. **51** (2013), 78–83.
62. R. Meštrović, *Wolstenholme's theorem: Its generalizations and extensions in the last hundred and fifty years (1862–2012)*, (2011), available at https://arxiv.org/abs/1111.3057.
63. R. Meštrović, *Lucas' theorem: Its generalizations, extensions and applications (1878–2014)*, (2014), available at https://arxiv.org/abs/1409.3820.
64. H. Ohtsuka, *Problem H-737*, Fibonacci Quart. **51**, 186.
65. G. Olive, *Generalized powers*, Amer. Math. Monthly **72** (1965), 619–627.
66. H. Pan, *A generalization of Wolstenholme's harmonic series congruence*, Rocky Mountain J. Math. **38** (2008), 1263–1269.
67. P. Phunphayap and P. Pongsriiam, *Explicit formulas for the p-adic valuations of Fibonomial coefficients*, J. Integer Seq. **21** (2018), Article 18.3.1.
68. P. Phunphayap and P. Pongsriiam, *Explicit formulas for the p-adic valuations of Fibonomial coefficients II*, AIMS Math. **5** (2020), no. 6, 5685–5699.
69. C. Pomerance, *Divisibility of the middle binomial coefficient*, Amer. Math. Monthly **122** (2015), 636–644.
70. J. Rosen, *Multiple harmonic sums and Wolstenholme's theorem*, Int. J. Number Theory **9** (2013), no. 8, 2033–2052.

71. B. Sagan and C. Savage, *Combinatorial interpretations of binomial coefficient analogues related to Lucas sequences*, Integers **10** (2010), 697–703.
72. C. Sanna, *Central binomial coefficients divisible by or coprime to their indices*, Int. J. Number Theory **14** (2018), 1135–1142.
73. Ling-Ling Shi, *Congruences for Lucas u-nomial coefficients modulo* p^3, Rocky Mountain J. Math. **37** (2007), 1027–1042.
74. J. Southwick, *A conjecture concerning the Fibonomial triangle*, (2016), available at https://arxiv.org/abs/1604.04775
75. R. P. Stanley, *Enumerative Combinatorics*, Volume 1. Second edition. Cambridge Studies in Advanced Mathematics, **49**. Cambridge University Press, 2012.
76. R. P. Stanley, *Catalan Numbers*, Cambridge University Press, New York, 2015.
77. R. Tauraso, *More congruences for central binomial coefficients*, J. Number Theory **130** (2010), 2639–2649.
78. J. Vinson, *The relation of the period modulo m to the rank of apparition of m in the Fibonacci sequence*, Fibonacci Quart. **1** (1963), 37–45.
79. M. Ward, *Note on divisibility sequences*, Bull. Amer. Math. Soc. **42** (1936), 843–845.
80. M. Ward, *A calculus of sequences*, Amer. J. Math. **58** (1936), no. 2, 255–266.
81. M. Ward, *The linear p-adic recurrence of order two*, Illinois J. Math. **6** (1962), 40–52.
82. D. L. Wells, *Lucas' Theorem for Generalized Binomial Coefficients*, Ph. D. thesis, Washington State University, 1992.
83. B. Wilson, *The Fibonacci triangle modulo p*, Fibonacci Quart. 36 (1998), no. 3, 194–203.
84. J. Wolstenholme, *On certain properties of prime numbers*, Q. J. Pure Appl. Math. **5** (1862), 35–39.

Chapter 6
Cubic Extensions of the Lucas Sequences

I don't think that everyone should become a mathematician, but I do believe that many students don't give mathematics a real chance. (Maryam Mirzakhami)

They never tell us how addictive mathematics can be. That's wrong. They really ought. (Overheard from a graduate student at the 2014 International Conference on Fibonacci Numbers)

Abstract This is the first of three chapters devoted to the question of how to generalize the Lucas sequences. We begin with a detailed discussion of Lucas's thoughts concerning this problem, one which he regarded as being of very great importance. This is followed by some historical commentary. As Lucas regarded linear recurrences as being key to providing an answer to this question, we first discuss the possible application of cubic linear recurrences to it. We then move on to several proposals for solutions, including Bell's ideas and Williams's suggestions and concluding with Roettger's remarkable sequences.

6.1 Lucas' Attempts to Generalize His Sequences

In several of his works on the (U_n) and (V_n) sequences, Lucas mentioned the problem of extending or generalizing them. In particular, he provided a lengthy discussion of this question in [15]. In what follows, we will present his arguments in [15] and some further remarks of Lucas, which are relevant to this topic. It should be pointed out that Lucas frequently repeated himself, so we will provide only one of any repeated statement. For more information concerning this subject, see Chap. 1 of Roettger [23].

© Springer Nature Switzerland AG 2023

C. J.-C. Ballot, H. C. Williams, *The Lucas Sequences*, CMS/CAIMS Books in Mathematics 8, https://doi.org/10.1007/978-3-031-37238-4_6

In Sect. I of his memoir [15], he states:

This memoir has as its objective the study of symmetric functions of the roots of an equation of the second degree, and its application to the theory of prime numbers. We will first show the complete analogy of these symmetric functions with the circular and hyperbolic functions. We then show the connection that exists between the symmetric functions and the theory of determinants, combinations, continued fractions, divisibility, divisors of quadratic forms, continued radicands, division of the circumference of the circle, indeterminate analysis of the second degree, quadratic residues, decomposition of large numbers into their prime factors, etc. This method is the point of departure of a more complete study, of the properties of the symmetric functions of the roots of an algebraic equation of any degree with rational coefficients, in their relation to the theories of elliptic and Abelian functions, of power residues, and indeterminate analysis of higher degrees.

In commenting later concerning [15], he added (see Lucas [16]):

Since the publication of this work, the author has added to it twenty other sections, as yet unpublished, which altogether form the arithmetical theory of the symmetric functions of the roots of equations of the second degree. The author hopes to find the time to write up in a similar manner the theory of doubly periodic functions, in their connection to symmetric functions of the roots of equations of the third and fourth degree, and with elliptic functions.

Lucas appeared to abandon this subject until 1891 when he circulated, prior to the Marseille meeting (Sept. 17–24) of the French Association for the Advancement of Science (AFAS), his most extensive commentary (Lucas [18]) concerning this problem. As this communication provides much information concerning his thoughts on this matter, we quote the relevant part of it in full:

But we think we should stress in a particular way research concerning linear recurring sequences [Lucas often uses the terms 'recurrence sequences' and 'linear recurrence sequences' as synonyms. (See, for example, Chap. XVII of [17].)] of various orders and its connection to the theory of elliptic and abelian functions. In several memoirs published in the *Comptes rendus de l'Association*, from the meetings in Clermont, Nancy, Paris and le Havre, in the *Actes de l'Académie royale des Sciences de Turin* and of Saint Petersburg, in the Nouvelle Correspondance mathématique, in the *Journal de Sylvester* in Baltimore [American Journal of Mathematics], etc., we have demonstrated the analogy and, as it were, the similarity of the circular and hyperbolic functions with the numerical functions of the second order, whose characteristic polynomials are of degree two. (See Chaps. XVII and XVIII in our book [17]). To every trigonometric formula corresponds a formula for these functions, and conversely.

We had hoped to find in this study, through the prime decomposition of the expressions $(a^n \pm b^n)$, a demonstration of Fermat's last theorem concerning the impossibility of solving in integers the indeterminate equation

$$x^p + y^p + z^p = 0$$

in which it suffices to assume that p denotes a prime. Although Kummer treated this equation masterfully a long time ago, it has still not been completely solved, as many of the exponents p cannot be dealt with by his admirable analysis.

But if this research plan has not up to now provided the solution of this celebrated problem, it does allow us to obtain a number of Wilsonian theorems, that is to say the necessary and sufficient conditions that a given p of twenty or thirty digits must satisfy to be prime when one knows the decomposition in prime factors of one of the numbers $p \pm 1$. Furthermore, this method guides us to the notion of periodicity of the residues for prime or composite moduli. Therefore, there is every reason to search for formulas analogous to the addition and multiplication formulas for the numerical functions which are derived from recurrences whose characteristic polynomials are of degree three and four. These formulas find their origin in the theory of elliptic functions, and we encounter some of them in a beautiful memoir of Moutard (1)

(1) Poncelet, Applications d'Analyse et de Géométrie, t. 1er, addit. III, p. 542–548.

[Moutard's paper appeared as a special section in Poncelet's book.]

One rediscovers these recurrence sequences by generalizing the theory of linear substitutions, described by Serret in his *Cours d'Algèbre supérieure* (4th edition, vol II, pp. 356-412) in a too-particular form. If one considers n linear homogeneous forms in n variables provided by the linear substitutions

$$\begin{aligned} x_{p+1} &= \lambda_1 x_p + \mu_1 y_p + \nu_1 z_p + \dots , \\ y_{p+1} &= \lambda_2 x_p + \mu_2 y_p + \nu_2 z_p + \dots , \\ z_{p+1} &= \lambda_3 x_p + \mu_3 y_p + \nu_3 z_p + \dots , \end{aligned}$$

.....,

in which the coefficients λ, μ, ν, ..., are constants, the forms x_{p+1}, y_{p+1}, z_{p+1}, ..., are expressed as functions of x, y, z,..., and the coefficients of the variables x, y, z, ..., producing linear sequences having for their characteristic equation

$$U = \begin{vmatrix} \lambda_1 - u & \mu_1 & \nu_1 & \dots \\ \lambda_2 & \mu_2 - u & \nu_2 & \dots \\ \lambda_3 & \mu_3 & \nu_3 - u & \dots \\ \dots & \dots & \dots & \dots \end{vmatrix} = 0,$$

in which u denotes the variable. The ratios of consecutive functions, or of coefficients corresponding to two consecutive functions, have for their limits under certain conditions of convergence, the root of largest modulus of the equation $U = 0$. One can therefore generalize in an infinitude of ways Bernoulli's approximation technique for calculating the roots of equations.

This method is developed in the first volume of Legendre's Théorie des nombres, but only for a very particular case.

In Addition X *Sur l'extraction des racines pour les moyennes* (p. 506) of our book, we have pointed out a new process for obtaining roots of any index.

This process also relates to the preceding theories and to linear substitutions. We think that, by developing these new methods, by searching for the addition and multiplication formulas of the numerical functions which originate from recurrence sequences of the third and of the fourth degree, and by studying in a general way the laws of the residues of these functions for prime moduli, according to how they look, their cubic or biquadratic character in relation to the discriminant of the equation $U = 0$, that we would arrive at important new properties of prime numbers. And perhaps the complete proof of Fermat's last theorem is just a consequence of the famous theorem of Jacobi concerning the impossibility of more than two periods for holomorphic functions of a single variable.

From this material, it appears that Lucas's investigations into his sequences were originally motivated by his earlier interest in Diophantine problems, particularly Fermat's last theorem. (See Lucas [14] and Chap. 1 for more on this topic.) In connection with this, we mention that Ballot [2] showed that the sequences (U_n), (V_n), where

$$\delta U_n = (c-b)a^n + (a-c)b^n + (b-a)c^n \quad \text{and} \quad V_n = a^n + b^n + c^n$$

with $\delta = (a-b)(b-c)(c-a)$ provide a weak, but natural, generalization of the Lucas sequences $((a^n - b^n)/(a-b))$ and $(a^n + b^n)$. Here a, b, c denote distinct, nonzero integers. He proved weak Lucas-like laws of appearance for certain special primes in an infinite set S and showed that if a certain subset T of S is infinite, then Fermat's last theorem would follow.

With regard to linear recurring sequences, Lucas wrote the following in the Introduction to his book [17]:

The theory of recurrent sequences is an inexhaustible mine which contains all the properties of numbers; by calculating the successive terms of such sequences, decomposing them into their prime factors and seeking out by experimentation the laws of appearance and reproduction of the prime numbers, one can advance in a systematic manner the study of the properties of numbers and their application to all branches of mathematics.

After Lucas' untimely death, there seemed to be little notice of the problem of generalizing his functions. His old friend, C.-A. Laisant tried to kindle some interest through a question in the journal, *L'Intermédiaire des mathématiciens* [12]:

We know how much the famous theorem of Fermat concerning the impossibility of the identity $x^n + y^n = z^n$, in integers, has so preoccupied mathematicians. We can no longer ignore that the greater part of the work of Éd. Lucas on the theory of numbers had for its object, direct or indirect,

the quest for a demonstration of this theorem. In particular, he published a very interesting memoir *Sur la théorie des fonctions numériques simplement périodiques*. These functions U_n and V_n arise from the equation of the second degree and present striking analogies with the sine and cosine functions.

In seeking to generalize these ideas, Lucas later sent a Communication to the Société mathématique de France, which unfortunately was not inserted, no Note having been put in by the author, on three numerical functions, arising from the equation of the third degree, offering very great analogies with the elliptic functions, and exhibiting the property of being doubly periodic.

Shortly after, during a conversation that I had with him, Lucas said to me: 'if one could establish that my doubly periodic functions only have two distinct periods, the theorem of Fermat would be proved.' And during a meeting, assuming this hypothesis, he justified his statement by a demonstration which was easy for me to follow, but of which I have totally lost any memory, being far from suspecting his approaching death. I recall only that the case of the exponent 2 was isolated, just as it should be, in a very precise manner.

It is possible that Lucas had made similar Communications to other colleagues, more favoured from the point of view of memory and more attentive than I had been. In this case, I make an appeal to them through the present question to consult their memories. It may also be possible that the members of the Société mathématique might be able to recover the three numerical functions of which I have spoken, and concerning which I have not found any indication in the papers left by the author. This would assuredly be a very interesting gap to fill.

Laisant amplified these remarks in response to a query from D. E. Smith in 1913 sent at the behest of E. T. Bell (Bell [5]):

The mathematical papers of Lucas, after his death, were entrusted to a commission of three members: M. Delannoy, Lemoine and myself. We found in them the necessary elements for the publication of the last two volumes (iii and iv) of the Récréations Mathématiques, and of the volume L'Arithmétique Amusante.

The remainder consisted of scattered notes which, in our estimation, were not available for publication... I found no trace of the subject about which you particularly enquire, and I regret it keenly. I had studied with great interest the memoir *Sur les fonctions numériques simplement périodiques*, and I often chatted over it with the author. These functions U, V, derived from the equation of the second degree present curious analogies with the sine and cosine. Lucas has also considered three functions derived from the equation of the third degree, on which he once made a communication to the Mathematical Society of France. I can find no trace of this communication, and I have lost all memory of it. I recall only the definition of one of these functions; it was $a^n + b^n + c^n$, a, b, c, being the roots of the equation. From the point of view of periodicity these functions exhibited the closest analogies

with *sn*, *cn*, *dn* of elliptic functions. They presented certain characters of double periodicity.

On examining the above material, we note several aspects of Lucas' exploration of his sequences and his analysis of those that he considered might be suitable generalizations of them. We certainly see that he was interested in functions satisfying linear recurrence sequences; these functions should be symmetric functions of the roots of an associated polynomial with rational (in practice, usually integral) coefficients; further, it seems that he was considering more than one function in this study. He also appears to have been particularly interested in functions linked to polynomials of degree three or four. Admittedly, it is difficult to determine in these cases when Lucas was referring to sequences satisfying a third- or fourth-order linear recurrence or to sequences whose terms are symmetric functions of the roots of a third- or fourth-degree polynomial; he mentions both. He emphasized the need to find addition and multiplication formulas involving these functions, as this was what he did in order to prove the many properties of his own functions of order 2. His suggested method of approach was to use empirical methods to attempt to elucidate what the laws of appearance and repetition for these functions would be, and from this material he should be able, as he did in the case of (U_n) and (V_n), to derive further properties of primes, such as primality testing algorithms. However, despite this possible program of research, he seems never to have produced any results that were analogous to his work on the Lucas functions.

In his memoir, he mentioned three different possible directions of approach; however, it seems that he regarded these as being aspects of a more general methodology involving the study of singly and doubly periodic functions. The first of these involved symmetric functions of the zeros α, β, γ of a cubic polynomial which also satisfy linear recurrences. In particular, Lucas considered the power sum $S_n = \alpha^n + \beta^n + \gamma^n$, for the characteristic polynomial $x^3 - x - 1$. This specific sequence (S_n) is now called the Perrin sequence, and was the focus of much attention by Adams and Shanks [1]; it seems first to have been considered by Catalan [6] in 1861. Catalan, who denoted the sequence by (A_n), believed that A_n is or is not divisible by n according to whether or not n is a prime. This could easily be converted into a primality test for N that would execute in polynomial time in $\log N$, but unfortunately, Catalan's assertion is untrue. For example, we see in [1] that $271441 (= 521^2)$ divides A_{271441}; furthermore, several other values of composite n such that $n \mid A_n$ are also provided in [1]. We should remark here that some of the work in [1] was later extended by Szekeres [28]. Also, Grantham[9] has shown that there exist infinitely many Perrin pseudoprimes, as conjectured in [1].

In Chap. 8 of her thesis, Décaillot [7] raised the interesting possibility that Lucas was aware of Catalan's work before he (Lucas) embarked on his work in primality testing and that it might have inspired him in his investigations. However, Lucas, who knew Catalan and who is usually most punctilious in assigning priority, nowhere mentions Catalan's work. Also, Lucas' result (see

Sect. XXI of [15]) concerning this matter (if $n \mid A_n$ and $n \nmid A_j$ for all j such that $0 < j < n$, then n is a prime) is more carefully stated than Catalan's, even though Lucas' proof of this result is incomplete. Perhaps Lucas did not want to embarrass Catalan by mentioning his less circumspect work or, more likely, he was simply unaware of [6].

Lucas' second suggestion was a study of the function:

$$U_n = \Delta(\alpha^n, \beta^n, \gamma^n, \cdots)/\Delta(\alpha, \beta, \gamma, \cdots), \tag{6.1}$$

where $\alpha, \beta, \gamma, \ldots$ denote the roots of an associated polynomial and $\Delta(\alpha, \beta, \gamma, \cdots)$, denotes the discriminant of that polynomial. He claimed that such a study would result in the generalization of the principal formulas contained in the first part of his memoir, but did not follow up on this idea. Lucas's third idea was motivated by the connection of the Lucas sequences to the singly periodic circular functions and by their periodic properties modulo m (see Sect. 4.1). It seems that from what little he did write on this matter that he believed an attempt to generalize his sequences could begin through an investigation of the properties of doubly periodic functions, such as the elliptic functions, and their connection with recurrent sequences. We will discuss his third suggestion in some detail in Sects. 8.1 and 8.2.

6.2 Cubic Linear Recurrences

As it appears that Lucas considered linear recurring sequences of order three, or cubic recurrences, to be key to the problem of extending of the Lucas sequences, we will discuss such sequences in this section. We have already noted his interest in the cubic recurrence sequence (A_n). We now examine the recurrence sequence (X_n), where P, Q, R are given integers and

$$X_{n+3} = PX_{n+2} - QX_{n+1} - RX_n, \quad \text{for } n \geq 0. \tag{6.2}$$

Let α, β, γ be the three roots of the characteristic polynomial:

$$f(x) = x^3 - Px^2 + Qx - R. \tag{6.3}$$

Since (6.2) is a homogeneous linear difference equation of degree three with constant coefficients, we know that if α, β, γ are distinct, then

$$X_n = c_1\alpha^n + c_2\beta^n + c_3\gamma^n, \tag{6.4}$$

for certain constants c_1, c_2, c_3. These constants can be determined from initial conditions on (X_n) such as the values of X_0, X_1, and X_2. In the case where only two of the roots of $f(x)$ are distinct, say $\alpha = \beta$ and $\gamma \neq \alpha$, then we replace (6.4) by

$$X_n = (c_1 n + c_2)\alpha^n + c_3\gamma^n;$$

when $\alpha = \beta = \gamma$, we replace (6.4) by

$$X_n = (c_1 n^2 + c_2 n + c_3)\alpha^n.$$

For an elementary introduction to the theory of difference equations, see, for example, the book of Goldberg [8]. All of this material was known to Lucas (see Chap. XVII of [17]), but it appears he was unable to find a particular set of third-order recurring sequences which was satisfactory. One of the main features of the (second-order) Lucas sequences is that U is a divisibility sequence (see Sect. 2.3), and much of the rich arithmetic theory of his sequences is dependent on this; however, it seems that the only third-order recurring sequences (X_n) which are also divisibility sequences are given by $X_n = n^2 a^{n-1}$, or $X_n = U_n^2$, where a is an integer and U_n is either a Lucas or Lehmer function. The arithmetic theory of these functions is essentially the same as that of the Lucas/Lehmer functions, and therefore they would not have served as an interesting or useful generalization of U. In [10] Hall showed that if (X_n) is a divisibility sequence and $X_0 \neq 0$, then the totality of the primes that can divide all terms of (X_n) is finite; indeed, these primes must divide the $\gcd(X_0, R)$. Thus, such a sequence is of limited interest. The following result was also proved by Hall in [10].

Theorem 105 (Hall [10]) *There is no divisibility sequence* (X_n) *with* $X_0 = 0$ *whose characteristic polynomial is an irreducible (over the rationals) cubic whose last two coefficients are relatively prime.*

Later Ward [30] eliminated the condition that the last two coefficients of $f(x)$ be coprime. In a footnote on page 580 of [10], Hall states that he learned from Ward that he (Ward) had shown that there could be no (interesting) divisibility sequence whose characteristic polynomial has a linear and an irreducible quadratic factor. However, it appears that either Hall or Ward might have been mistaken in this assertion because Ward makes no reference to this result in any of his papers, particularly where this result would have been very relevant to his theme. See, for example, p. 88 of [30].

It seems, then, that it is unlikely that there exist any interesting divisibility sequences of order three, but it must be stressed here that so far this has not been proved. Certainly no such sequence has been found up to now. Given Lucas' use of empirical methods, he might have discovered that using third-order linear sequences would not provide a fruitful avenue of discovery, but see the remarks at the end of Sect. 7.2. Nevertheless, Ward [30] was able to develop laws of repetition and appearance for primes in a general cubic recurrence; however, it is questionable as to whether these were the kind of results that Lucas was seeking, as he seems to have been concerned with particular sets of sequences satisfying (6.2).

6.3 Bell's Contribution

On reading Laisant's letter, E.T. Bell [5] developed an interest in the problem of extending the Lucas sequences to third-order recurrences. In the Lucas sequence case, we observe that there must exist integer sequences (X_n) and (Y_n) for $n \geq 0$ such that

$$\alpha^n = Y_n\alpha + X_n, \tag{6.5}$$

where $X_0 = 1, Y_0 = 0, X_1 = 0, Y_1 = 1$. Since β is also a root of $x^2 - Px + Q$, we see that (6.5) must hold when we substitute β for α. From the resulting two equations, it is easy to deduce that $V_n(P, Q) = 2X_n + PY_n$ and $U_n(P, Q) = Y_n$. Notice that we have the formulas:

$$\begin{aligned} \alpha^{m+n} &= Y_{m+n}\alpha + X_{m+n} = (Y_m\alpha + X_m)(Y_n\alpha + X_n) \\ &= \alpha(PY_mY_n + X_mY_n + Y_mX_n) + X_mX_n - QY_mY_n, \end{aligned} \tag{6.6}$$

and

$$\alpha^{mn} = Y_{mn}\alpha + X_{mn} = (Y_n\alpha + X_n)^m, \tag{6.7}$$

which can be used to find the addition and multiplication formulas for (X_n) and (Y_n).

This appears to provide an avenue of approach to the problem of extending the Lucas sequences. We now let α, β, γ be the three roots of (6.3) and define, as did Bell, the integer sequences (x_n), (y_n), (z_n) for $n \geq 0$

$$\alpha^n = z_n\alpha^2 + y_n\alpha + x_n. \tag{6.8}$$

with similar expressions for β and γ. In this case we have $x_0 = 1$, $y_0 = 0$, $z_0 = 0$; $x_1 = 0$, $y_1 = 1$, $z_1 = 0$; $x_2 = 0$, $y_2 = 0$, $z_2 = 1$. Also, each of the three sequences (x_n), (y_n), (z_n) satisfies the recurrence (6.2), and each of x_n, y_n, z_n can be written as a symmetric function of α, β, γ. Unfortunately neither is $S_n = \alpha^n + \beta^n + \gamma^n$, but we can write S_n as a simple linear combination of x_n, y_n, and z_n: $S_n = (P^2 - 2Q)z_n + Py_n + 3x_n$; indeed, we can write any particular integral sequence satisfying (6.2) as a linear combination (with fixed integral coefficients) of x_n, y_n, and z_n. It is easy to see that the sequences (V_n) and (U_n) defined in Ballot [2] are given by $V_n = S_n$ and $U_n = z_n$.

Further properties of *Bell's sequences* have been derived by Ward [29], Mendelsohn [19], and Müller [20]. In the latter paper, it is shown how they can be used to produce a fast algorithm for solving the cubic congruence $x^3 \equiv m \pmod{p}$, where p is a prime such that $9 \mid p - 1$ and the integer m is a cubic residue of p. (See Sect. 3.4.) We should also mention that Lucas himself discusses these sequences in more general context in Sect. 173 of [17]. For suppose we put

$$f(x) = x^k - P_1x^{k-1} + P_2x^{k-2} - \cdots + (-1)^kP_k, \tag{6.9}$$

where $P_1, P_2, \ldots, P_k$ are fixed given integers. If ρ_i is any of the k roots of (6.9), then by complete analogy to (6.8), we can write

$$\rho_i^n = Z_{k-1,n}\rho_i^{k-1} + Z_{k-2,n}\rho_i^{k-2} + \cdots + Z_{0,n}.$$

Here we see that $Z_{i,j} = \delta_{i,j}$ $(0 \le i, j < k)$, where $\delta_{i,j} = 0$ when $i \ne j$ and $\delta_{i,i} = 1$; also, $Z_{i,k} = (-1)^{k-i+1}P_{k-i}$. Furthermore, by analogy to (6.2), we get:

$$Z_{i,n+k} = P_1 Z_{i,n+k-1} - P_2 Z_{i,n+k-2} + \cdots + (-1)^{k-1}P_k Z_{i,n}.$$

Notice that if $f(x) = x^2 - Px + Q$, we get $X_n = Z_{0,n}$, $Y_n = Z_{1,n}$; if $f(x)$ is given by (6.3), then $x_n = Z_{0,n}$, $y_n = Z_{1,n}$ and $z_n = Z_{2,n}$.

In Sect. 173 of [17], using a different notation, Lucas simply mentions the k sequences $(Z_{i,n})$ for $i = 0, 1, 2, \ldots, k-1$ without much additional comment. If these were the sequences that he was thinking about as a possible solution to the problem of extending the Lucas sequences, it seems odd that he did not say anything further.

We see that we can use results like (6.6) and (6.7) to find addition and multiplication formulas for x_n, y_n, and z_n; indeed, we have:

$$z_{mn}\alpha^2 + y_{mn}\alpha + x_{mn} = (z_n\alpha^2 + y_n\alpha + x_n)^m. \tag{6.10}$$

In commenting on a formula which is essentially (6.10), Bell concluded [4] with the following comment:

We reach here an essential difficulty of the whole subject [order three recurrence versions of Lucas' sequences], that is, the determination in a *practicable form* [Bell's italics] of z_{mn}, y_{mn}, x_{mn} from the identity of definition [(6.10)]. The corresponding problem for Lucas's functions presents no difficulty and much of the arithmetic fertility of his theory springs directly from the ease with which the complete solution is found in his case and the consequent simplicity of the resulting functions. This simplicity vanishes, apparently irrevocably, when we pass beyond second order series.

In retrospect, this verdict seems unduly pessimistic, but it explains Bell's subsequent abandonment of the recurring sequence method of approach to Lucas' problem of generalization.

6.4 The Cubic Pell Equation

Let ζ_n denote a primitive nth root of unity (see Sect. 4.3). For example, when $n = 2$, $\zeta_n = -1$ and when $n = 3$, ζ_n and ζ_n^2 (ζ_n^{-1}) are the two roots of the quadratic equation: $x^2 + x + 1 = 0$. We remark that the Pell equation (3.14) can be written as

$$x^2 - dy^2 = (x + \sqrt{d}y)(x + \zeta_2\sqrt{d}y) = 1.$$

Set $\delta = \sqrt[3]{d}$. The cubic version of the Pell equation can now be written as

$$x^3+dy^3+d^2z^3-3dxyz = (x+\delta y+\delta^2 z)(x+\omega\delta y+\omega^2\delta^2 z)(x+\omega^2\delta y+\omega\delta^2 z) = 1, \tag{6.11}$$

where $\omega = \zeta_3$. For an elementary introduction to this Diophantine equation, see Chap. 7 of [4]; for a more advanced treatment and several references, see Chap. 5 of Hambleton and Williams [11]. The behavior of the solutions of (6.11) is very similar to that of the solutions of the Pell equation, in that if d is not a perfect integral cube, there always exists a fundamental solution (X_1, Y_1, Z_1) of (6.11) from which all other solutions can be derived. The determination of the fundamental solution is a rather intricate process for most values of d, but Rudman [26], completing earlier work of Nagell and Stender (see [26] for references), showed that whenever d has the parametric form $d = M^3 + k$, where $k \mid 3M^2$, then it is a simple matter to find the fundamental unit η (< 1) of the pure cubic field $\mathbb{Q}(\delta)$. In almost all cases $\eta = (\delta - M)^3/k$. If we we apply his results in the particular case of $k \mid 3M$, we usually $(|k| \neq 1)$ have the fundamental unit of the ring $Z[\delta]$ as $\eta = (\delta - M)^3/k$ or

$$k^2\eta^{-1} = 9M^6 + 9M^3k + k^2 + (9M^5 + 6M^2k)\delta + (9M^4 + 3Mk)\delta^2.$$

For example, if $d = M^3 + \epsilon$, where $\epsilon = \pm 1$, then, Nagell showed that we can put $X_1 = M^2$, $Y_1 = M$, $Z_1 = 1$, but if $d = M^3 + 3\epsilon$, then we put $X_1 = M^6 + 3\epsilon M^3 + 1$, $Y_1 = M^5 + 2\epsilon M^2$, $Z_1 = M^4 + \epsilon M$.

If we put $\alpha = X_1 + \delta Y_1 + \delta^2 Z_1$, $\beta = X_1 + \omega^2\delta Y_1 + \omega\delta^2 Z_1$ and $\gamma = X_1 + \omega\delta Y_1 + \omega^2\delta^2 Z_1$, then any integer solution of (6.11) can be written as (X_n, Y_n, Z_n) for some integer n, where

$$X_n+\delta Y_n+\delta^2 Z_n = \alpha^n,\ X_n+\omega^2\delta Y_n+\omega\delta^2 Z_n = \beta^n,\ X_n+\omega\delta Y_n+\omega^2\delta^2 Z_n = \gamma^n.$$

From these equations, we can easily deduce that

$$\begin{aligned} 3X_n &= \alpha^n + \beta^n + \gamma^n, \\ 3\delta Y_n &= \alpha^n + \omega\beta^n + \omega^2\gamma^n, \\ 3\delta^2 Z_n &= \alpha^n + \omega^2\beta^n + \omega\gamma^n. \end{aligned} \tag{6.12}$$

Notice that α, β, γ are the roots of the cubic polynomial $x^3 - 3X_1x^2 + 3(X_1^2 - dY_1Z_1)x - 1$; hence, the sequences (X_n), (Y_n), (Z_n) all satisfy the third-order linear recurrence (6.2) with $P = 3X_1$, $Q = 3(X_1^2 - dY_1Z_1)$, and $R = 1$.

6.5 Williams's Sequences

On referring back to (2.4), we can produce an alternative definition of the Lucas sequences (U_n) and (V_n) by first putting, for given integers P and D, $\alpha = (P + \delta)/2$, $\beta = (P - \delta)/2$, where $\delta^2 = D$. We then define:

$$U_n = \frac{\alpha^n - \beta^n}{\delta}, \quad V_n = \alpha^n + \beta^n.$$

We then have $U_1 = 1$, $V_1 = P$. In [31], Williams made use of this definition and (6.12) in order to produce a cubic extension of the Lucas functions. For integers P, Q, R ($\neq 0$), D, let α, β, γ be the roots of the polynomial (6.3) and $\delta^3 = D$. We define:

$$W_n = \alpha^n+\beta^n+\gamma^n, \quad V_n = (\alpha^n+\omega\beta^n+\omega^2\gamma^n)/\delta, \quad U_n = (\alpha^n+\omega^2\beta^n+\omega\gamma^n)/\delta^2,$$

subject to the constraint that W_n, V_n, U_n all be integers for all $n \geq 0$. Note that we now are using the notation (U_n) and (V_n) to refer to these new sequences, not the standard Lucas sequences. Naturally, this constraint leads to a priori conditions that have to be satisfied by P, Q, R, and D, and these are provided in Chap. 4 of [31]. It is important to observe that, unlike the case of the Lucas sequences, the sequences (W_n), (V_n), (U_n) $(n \geq 0)$ cannot all be integral for any choice of the integers P, Q, R. This is because the functions W_n, V_n, U_n are not symmetric functions of α, β, γ. For the P, Q, R selected as above, it is easy to show that W_n, V_n, U_n are related to the corresponding Bell sequences by $W_n = x_n/3$, $V_n = y_n/3$, $U_n = z_n/3$.

For given complex numbers a, b, put $\Phi_1 = \omega a - \omega^2 b$ and $\Phi_2 = \omega^2 a - \omega b$. We define $R_n = (\omega^2\Phi_1^n - \omega\Phi_2^n)/(\omega^2 - \omega)$, $S_n = (\omega\Phi_1^n - \omega^2\Phi_2^n)/(\omega^2 - \omega)$, $T_n = (\Phi_1^n - \Phi_2^n)/(\omega^2 - \omega)$. In Chap. 3 of [31], it is shown that if we put $L_m = W_m + \omega V_m + \omega^2 U_m$, $a = \omega^2 U_m - W_m$, $b = W_m - \omega V_m$, then

$$3^n W_{mn} = L_m^n+R_n-S_n,\ 3^n\omega V_{mn} = L_m^n+T_n-R_n,\ 3^n\omega^2 U_{mn} = L_m^n+S_n-T_n.$$

Many identity properties of R_n, S_n, T_n are presented in [31], and in [34] further arithmetic properties are derived for the case in which $a - b$ and $a^2 + ab + b^2$ are both integers. These results were extended and generalized by Ballot in [3].

Just as in the case of the Lucas sequences, the sequences (W_n), (V_n), (U_n) satisfy a number of algebraic identities, and it is possible to derive subtraction, addition, and multiplication formulas for each of them. However, since each of these sequences satisfies the third-order linear recurrence (6.2), we would not expect any of them to be a divisibility sequence. Nevertheless, this difficulty can be overcome by simply considering $D_n = \gcd(V_n, U_n)$. While the sequence (D_n) is not a linear recurrence sequence, it is a divisibility sequence, and many arithmetic properties of these extended Lucas sequences can be derived by making use of this observation and subsequent results concerning V_n and U_n modulo a prime. In this way, we can derive a law of appearance, a law of repetition, and a version of Lucas' fundamental theorem. Also, it is possible to employ these sequences to produce some primality tests. Indeed, all of Lucas' arithmetic results about his sequences have analogues in the realm of (W_n), (V_n), (U_n).

Also, Pocklington [22] made use of a special case ($D = m$, $W_1 = 3w_1$, $V_1 = 3v_1$, $U_1 = 3u_1$, where $R = w_1^3 + mv_1^3 + m^2u_1^3 - 3w_1v_1u_1$ is not a cubic residue of p) of these sequences to solve the cubic congruence $x^3 \equiv m \pmod{p}$, where p is a prime congruent to 1 modulo 3 and m is a cubic residue of p. The technique can be readily deduced from the triplication formulas for W_n, V_n, U_n and the result that $p \mid D_{p-1}$ whenever $p \equiv 1 \pmod{3}$ and D is a cubic residue of p. Pocklington's idea was extended in Williams [32] to the solution of the general binomial congruence $x^q \equiv m \pmod{p}$, where p and q are primes, q is odd and $q \mid p - 1$. This required sequences which were generalizations of the sequences (W_n), (V_n), (U_n), and the method represents an extension of the Cipolla technique discussed in Sect. 3.4. It was shown in Williams [33] that such sequences also share many of the same identity and arithmetic properties as the original Lucas sequences. The method of [32] was later improved by Williams and Hardy [35]. We also mention that Said and Loxton [27] have employed the Williams sequences to produce a cubic analogue, similar in concept to LUC, of the RSA cryptosystem.

While it may appear, then, that the sequences described above might have been what Lucas was seeking, it is unlikely that this extension of his functions would have been acceptable to him. While these sequences do satisfy a linear recurrence of order three, they are not symmetric functions of the zeros of the characteristic polynomial $f(x)$, and therefore they are not always integers unless the coefficients of $f(x)$ possess certain special properties.

6.6 Roettger's Sequences

One of the earliest attempts to extend the Lucas functions was done in 1880 by de Longchamps [13]. If we put $R = \alpha\beta\gamma$, where α, β, γ are the zeros of a cubic polynomial $f(x)$, Longchamps regarded D_n, E_n, and S_n, where

$$\begin{aligned} R^n D_n &= (\alpha^n + \beta^n)(\beta^n + \gamma^n)(\gamma^n + \alpha^n), \\ R^n E_n &= (\alpha^n - \beta^n)(\beta^n - \gamma^n)(\gamma^n - \alpha^n)/(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha), \\ S_n &= \alpha^n + \beta^n + \gamma^n, \end{aligned}$$

as the degree three functions analogous to the Lucas functions. Are these the three functions that Laisant mentioned? They are symmetric functions of α, β, γ, and they would have been known to Lucas because he was the Session Chair for the talk in which Longchamps presented his results. Also, as we mentioned at the end of Sect. 6.1, Lucas had already mentioned a general version of the function $\Delta(\alpha^n, \beta^n, \gamma^n, \cdots)/\Delta(\alpha, \beta, \gamma, \cdots)$ which, in the cubic case, Longchamps denoted by $R^n E_n$. In fact Longchamps showed how to express D_n and E_n in terms of the coefficients of $f(x)$. However, Lucas would not likely have been keen on the fact that the first two of these

functions would not necessarily be integral, but this is a minor difficulty which can be easily overcome.

In [23] (see, alternatively, Müller et al. [21]) Roettger began with a cubic polynomial $f(x) = x^3 - Px^2 + Qx - R$, where P, Q, R are integers and put

$$\delta = (\alpha-\beta)(\beta-\gamma)(\gamma-\alpha),\ \Delta = \delta^2 = P^2Q^2 - 4Q^3 - 4RP^3 + 18PQR - 27R^2,$$

where α, β, γ are the zeros of $f(x)$. Note that here Δ denotes the discriminant of $f(x)$, a cubic polynomial. We will assume here that $\delta \neq 0$. He next defined functions that we will denote here by U_n or $U_n(P,Q,R)$ and W_n or $W_n(P,Q,R)$—in this section we will confine the notation U_n, W_n to Roettger's functions only—as

$$\begin{aligned}\delta U_n &= (\alpha^n - \beta^n)(\beta^n - \gamma^n)(\gamma^n - \alpha^n)\\ &= (\alpha^n\beta^{2n} + \beta^n\gamma^{2n} + \gamma^n\alpha^{2n}) - (\alpha^{2n}\beta^n + \beta^{2n}\gamma^n + \gamma^{2n}\alpha^n),\\ W_n &= (\alpha^n\beta^{2n} + \beta^n\gamma^{2n} + \gamma^n\alpha^{2n}) + (\alpha^{2n}\beta^n + \beta^{2n}\gamma^n + \gamma^{2n}\alpha^n).\end{aligned}$$

We have $U_0 = 0$, $U_1 = 1$, $U_2 = PQ - R$; $W_0 = 6$, $W_1 = PQ - 3R$, $W_2 = P^2Q^2 - 2Q^3 - 2RP^3 + 4PQR - 3R^2$. Also, $U_{-n} = -R^{-2n}U_n$ and $W_{-n} = R^{-2n}W_n$, results analogous to (2.7).

Note that U_n is the same as Lucas' $\Delta(\alpha^n, \beta^n, \gamma^n, \cdots)/\Delta(\alpha, \beta, \gamma, \cdots)(= R^nE_n)$ and $W_n = V_n - 2R^n$, where

$$V_n = R^nD_n = (\alpha^n + \beta^n)(\beta^n + \gamma^n)(\gamma^n + \alpha^n).$$

Both U_n and W_n are symmetric functions of α, β, γ and are therefore integers for all nonnegative values of n. It is these functions that we will use as our extensions of the Lucas functions U_n and V_n. Observe that (U_n) is a divisibility sequence. However, both the sequences (U_n) and (W_n) satisfy the 6th-order recurrence:

$$X_{n+6} = A_1X_{n+5} - A_2X_{n+4} + A_3X_{n+3} - A_4X_{n+2} + A_5X_{n+1} - A_6X_n, \quad (6.13)$$

where $A_1 = PQ - 3R$, $A_2 = RP^3 + Q^3 - 5PQR + 6R^2$, $A_3 = R(P^2Q^2 - 2Q^3 - 2RP^3 + 6PQR - 7R^2)$, $A_4 = R^2A_2$, $A_5 = R^4A_1$, $A_6 = R^6$.

It seems odd that Lucas does not seem to have examined these sequences except, perhaps, in a very cursory manner. Possibly, considering his apparent fixation with third- and fourth-order recurrences, he was put off by (6.13). If so, he made a mistake, because the theory of the sequences (U_n) and (W_n) exactly parallels that of the Lucas sequences, even down to the Euler criterion (Theorem 36). There are addition formulas, multiplication formulas, and a number of identity relations. For example,

$$U_{2n} = U_n(W_n + 2R^n), \quad 2W_{2n} = \Delta U_n^2 + W_n^2 - 4R^nW_n$$

are the analogues of the Lucas duplication formulas (2.23) and (2.24) and

$$4U_{3n} = U_n(\Delta U_n^2+3W_n^2), \quad 4W_{3n} = W_n^2(W_n-6R^n)+3\Delta U_n^2(W_n+2R^n)+24R^{3n}$$

are the triplication formulas.

Furthermore, there is a rich arithmetic theory, including laws of repetition and appearance, which leads to new primality testing criteria. For example, if $L_n = 3^{2n+1} - 3^{n+1} + 1$ is known to be a prime, then a test can be derived for the primality of $N_n = 3^{n+1} - 2$. While rare, such prime pairs (L_n, N_n) do exist. These sequences can also be used to produce (Roettger and Williams [25]) sufficient and necessary tests for the primality of numbers N when $N^2 + N + 1$ is divisible by a large power of a prime.

Much of this is discussed in considerable detail in [23], to which the interested reader is directed. What is particularly remarkable in this system is that, just as in the case of the Lucas sequences, only the two sequences (U_n) and (W_n) are required for its development. In view of (6.13) and results in the next chapter, this seems to be most remarkable, as one would expect that more sequences might be needed. (According to Laisant, even Lucas expected to need three sequences in the cubic case.) In addition, it is argued in [23] that Lucas possessed the mathematical knowledge and ability needed to discover these results.

We conclude this section by pointing out that it is even possible to establish a public-key cryptosystem (Roettger and Williams [24]) through the use of these sequences.

References

1. W. Adams and D. Shanks, *Strong primality tests that are not sufficient*, Math. Comp. **39** (1982), 255–300.
2. C. Ballot, *A weak generalization of ordinary Lucas sequences involving the sequence* $\{A^N + B^N + C^N\}_{N\geq 0}$, Congr. Numer. **194** (2009), 39–44.
3. C. Ballot, *Lucas sequences with cyclotomic root field*, Dissertationes Math. **409** (2013), 92pp.
4. E. J. Barbeau, *Pell's Equation*, Springer, NY, 2003.
5. E. T. Bell, *Notes on recurring series of third order*, Tohoku Math. J. **24** (1924), 168–184.
6. E. Catalan, *Communication de théorie des nombres*, 6 avril 1861, Société Philomathique de Paris, Extraits des procès-verbaux des séances pendant l'année 1861, Paris, 1861, p. 49.
7. A.-M. Décaillot, *Édouard Lucas (1842–1891): le parcours original d'un scientifique français dans le deuxième moitié du XIX-ième siècle*, Ph. D. Thesis, Université René Descartes-Paris V, 1999.

8. S. Goldberg, *Introduction to Difference Equations*, Dover Publications, N.Y., 1986.
9. J. Grantham, *There are infinitely many Perrin pseudoprimes*, J. Number Theory **130** (2010), no. 5, 1117–1128.
10. M. Hall, *Divisibility sequences of the third order*, Amer. Journal Math. **58** (1936), 577–584.
11. S. A. Hambleton and H. C. Williams, *Cubic Fields with Geometry*, Springer Nature Switzerland AG, 2018.
12. C.-A. Laisant, *Question 744*, L'Intermédiaire des Mathématiciens **3** (1896), 33–34.
13. G. de Longchamps, *Sur les fonctions récurrentes du troisième degré*, Assoc. Française pour l'Avancement des Sciences, Compte rendu des sessions **9** (1880), 115–117.
14. É. Lucas, *Recherches sur l'analyse indéterminée et arithmétique de Diophante*, Bulletin de la Société d'émulation du Département de l'Allier **12** (1873), 441–532.
15. É. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. of Math. **1** (1878), 184–240, 289–321.
16. É. Lucas, *Notice sur les Titres et Travaux Scientifiques de M. Édouard Lucas*, D. Jouaust, Paris, 1880.
17. É. Lucas, *Théorie des Nombres*, Éditions Jacques Gabay, Paris, 1991 (Authorized re-edition of the original 1891 Gauthier-Villars edition.)
18. É. Lucas, *Questions proposées à la discussion des 1re et 2e sections, 1° Questions d'arithmétique supérieure*, Assoc. Française pour l'Avancement des Sciences, Compte rendu des sessions **20** (1891), 149–151.
19. N. S. Mendelsohn, *Congruence relationships for integral recurrences*, Canadian Math. Bull. **5** (1962), 281–284.
20. S. Müller, *On the computation of cube roots modulo p*, High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams, Fields Inst. Communications **41**, American Math, Society, Providence RI, 2004, pp. 293–304.
21. S. Müller, E. Roettger, and H. C. Williams, *A cubic extension of the Lucas functions*, Ann. Sci. Math. Québec **33** (2009), 185–224.
22. H. C. Pocklington, *The direct solution of the quadratic and cubic binomial congruences with prime moduli*, Proc. Camb. Phil. Soc. **19** (1917), 57–59.
23. E. Roettger, *A cubic extension of the Lucas functions*, Ph. D. Thesis, University of Calgary, 2009, available at https://prism.ucalgary.ca/handle/1880/103553
24. E. Roettger and H. C. Williams, *Public-key cryptography based on a cubic extension of the Lucas functions*, Fundamenta Informaticae **114** (2012), 325–344.

25. E. Roettger and H. C. Williams, *Some primality tests constructed from a cubic extension of the Lucas functions*, Fibonacci Quart. **59** (2021), 194–213.
26. R. J. Rudman, *On the fundamental unit of a purely cubic field*, Pacific J. Math. **46** (1973), 253–256.
27. M. R. Said and J. Loxton, *A cubic analogue of the RSA cryptosystem*, Bull. Australian Math. Soc. **68** (2003), 21–38.
28. G. Szekeres, *High order pseudoprimes in primality testing*, Paul Erdős is Eighty, Bolyai Soc. Math. Stud. **2** (1986), 451–458.
29. M. Ward, *The algebra of recurring series*, Annals of Math. (2) **32** (1931), 1–9.
30. M. Ward, *The laws of apparition and repetition of primes in a cubic recurrence*, Transactions Amer. Math. Soc. **79** (1955), 72–90.
31. H. C. Williams, *A generalization of the Lucas functions*, Ph. D. Thesis, University of Waterloo, 1969.
32. H. C. Williams, *Some algorithms for solving* $x^q \equiv N \pmod{p}$, Proc. 3rd S-E Conf. Combinatorics, Graph Theory and Computing, 1972, 451–462.
33. H. C. Williams, *On a generalization of the Lucas functions*, Acta Arith. **20** (1972), 33–51.
34. H. C. Williams, *Some properties of a special set of recurring sequences*, Pacific J. Math. **77** (1978), 273–285.
35. K. S. Williams and K. Hardy, *A refinement of H.C. Williams' qth root algorithm*, Math. Comp. **61** (1993), 475–483.

Chapter 7
Linear Recurrence Sequences and Further Generalizations

Cerveau : l'instrument, bien sûr, se détériore, mais on en joue plus habilement. (Jean Rostand)

Le mieux est l'ennemi du bien. (French proverb)

Abstract In this chapter we examine the problem of generalizing Lucas' sequences from the perspective of linear recurrences. We first derive a number of features of such recurrences, culminating in a generalization of Lucas' law of appearance. We follow this with an investigation of the properties of impulse sequences, particular cases of the more general linear recurrence. It turns out that the impulse sequences have many characteristics in common with the Lucas sequences. We next turn to the problem of generalizing the Lehmer sequences and how they may be used to produce necessary and sufficient tests of primality for numbers N of the form $N = Ap^n + \gamma$, where p is an odd prime, $2 \mid A$, $p \nmid A$, $\gamma \in \{1, -1\}$ and $A < p^n$.

7.1 Linear Recurrence Sequences

In this section we will consider some of the properties of linear recurrence sequences with constant integer coefficients. As we have seen in Sect. 6.1, these seemed to be the sequences that Lucas considered as essential to solving the problem of generalizing his sequences. We begin by generalizing some of the results in Sect. 4.1. Let k be a fixed positive integer and let the sequence (X_n) be determined by an initial vector of k integer values:

$$T_0 = (X_0, X_1, X_2, \ldots, X_{k-1}) \tag{7.1}$$

© Springer Nature Switzerland AG 2023

C. J.-C. Ballot, H. C. Williams, *The Lucas Sequences*, CMS/CAIMS Books in Mathematics 8, https://doi.org/10.1007/978-3-031-37238-4_7

and the kth-order linear recurrence

$$X_{n+k} = P_1 X_{n+k-1} - P_2 X_{n+k-2} + \cdots + (-1)^{k-1} P_k X_n, \tag{7.2}$$

where $P_1, P_2, \ldots, P_k$ are given fixed integers. Notice that the values for X_n for all $n \geq 0$ are completely determined by (7.1) and (7.2). We define the *characteristic polynomial* $f(x)$ of the linear recurring sequence (X_n) to be

$$f(x) = x^k - P_1 x^{k-1} + P_2 x^{k-2} - \cdots + (-1)^k P_k. \tag{7.3}$$

We define the *order* of (X_n) to be the least positive value of k such that (X_n) satisfies a relation of the type (7.2). If (X_n) is a linear recurring sequence, we say, following Ward [13], that an integer m (> 1) is a *null divisor* of (X_n) if for some minimal h (> 0), we have $m \mid X_n$ for all $n \geq h$. If (X_n) has no null divisors, it is said to be a *non-null sequence*. For example, a regular Lucas sequence U is always non-null. Observe that necessary conditions for (X_n) to be non-null are that $\gcd(X_0, X_1, X_2, \ldots, X_{k-1}) = 1$ and $\gcd(P_1, P_2, \ldots, P_k) = 1$, but these conditions are not in general sufficient.

For $i \geq 0$, let T_i denote the k-entry row vector $(X_i, X_{i+1}, X_{i+2}, \cdots, X_{i+k-1})$ and observe by (7.2) that $T_{i+1} = T_i C$, where C is the $k \times k$ companion matrix of $f(x)$. From this it follows by induction that $T_n = T_0 C^n$. We now assume that m is a fixed positive integer. Since there are only a finite number of residues of the integers modulo m, there must exist some r (> 0) and s (≥ 0) such that $C^{r+s} \equiv C^s \pmod{m}$; hence, $T_{r+s} \equiv T_s \pmod{m}$. Notice that the values of r and s here are independent of the initial conditions T_0. Since for any $i \geq 0$, $T_{i+1} \pmod{m}$ depends only on $T_i \pmod{m}$, we must have

$$T_i \equiv T_{i+r} \pmod{m} \quad \text{for all } i \geq s.$$

That is, there must exist some τ $(= \tau(m))$ such that $\tau \geq 1$ and

$$X_{n+\tau} \equiv X_n \pmod{m} \tag{7.4}$$

for all sufficiently large integers n. Notice that if (7.4) holds for all sufficiently large values of n, then $X_{n-\tau} \equiv X_n \pmod{m}$ must also hold for all sufficiently large values of n. As the determinant of C is P_k, we see that if $\gcd(m, P_k) = 1$, we have $C^r \equiv I \pmod{m}$, where I is the $k \times k$ identity matrix. Thus, in the particular case when $\gcd(m, P_k) = 1$, we see that (7.4) will hold for all $n \geq 0$ and $X_{n-\tau} \equiv X_n \pmod{m}$ for all $n \geq s$. We will now assume that τ is the least positive integer satisfying (7.4); we call τ the *minimal period length of* (X_n) *modulo* m. Observe that if t is any positive integer, then $X_{n-t\tau} \equiv X_n \pmod{m}$ for all $n \geq s$.

Suppose that for some integer $\omega \geq 1$, we have:

$$X_{n+\omega} \equiv X_n \pmod{m},$$

for all sufficiently large $n \geq 0$. By the same reasoning as that employed in Sect. 4.1, we see that we must have $\tau \mid \omega$.

Theorem 106 *If m_1 and m_2 are coprime positive integers, then $\tau(m_1 m_2) = \text{lcm}(\tau(m_1), \tau(m_2))$.*

Proof Set $\mu = \text{lcm}(\tau(m_1), \tau(m_2))$. By the previous observation, we must have $\tau(m_1) \mid \tau(m_1 m_2)$ and $\tau(m_2) \mid \tau(m_1 m_2)$; hence, $\mu \mid \tau(m_1 m_2)$. Also, since $\tau(m_1) \mid \mu$ and $\tau(m_2) \mid \mu$, we must have $X_i \equiv X_{i+\mu} \pmod{m_1}$ and $X_i \equiv X_{i+\mu} \pmod{m_2}$; hence, since m_1 and m_2 are coprime, we get $X_i \equiv X_{i+\mu} \pmod{m_1 m_2}$. It follows that $\tau(m_1 m_2) \mid \mu$, and therefore $\mu = \text{lcm}(\tau(m_1), \tau(m_2))$. □

We next examine the particular sequence (Z_n) which satisfies (7.2) with initial condition vector $(0, 0, 0, \ldots, 0, 1)$. This sequence is the same as $(Z_{k-1,n})$ in Sect. 6.3. For this specific sequence, we will denote the minimal period length of (Z_n) modulo m by $\pi(m)$. That is, for all sufficiently large n, we have

$$Z_{n+\pi} \equiv Z_n \pmod{m}. \tag{7.5}$$

Put $S_i = (Z_i, Z_{i+1}, Z_{i+2}, \ldots, Z_{i+k-1})$ and consider the $k \times k$ matrix M whose jth row is S_{j-1} for $j = 1, 2, \ldots, k$. We see that the rows of M can be permuted to form an upper triangular matrix with diagonal entries all 1. Thus, $\det(M) = \pm 1$ and the entries of M^{-1} are all integers. Put $B = T_0 M^{-1}$ and let $B = (b_0, b_1, b_2, \ldots, b_{k-1})$, where the b_i values are all integers. By definition of B, we have $T_n = T_0 C^n = BMC^n$, and since the jth row of MC^n is S_{n+j-1}, we see that MC^n is symmetric and

$$X_n = b_0 Z_n + b_1 Z_{n+1} + b_2 Z_{n+2} + \ldots + b_{k-1} Z_{n+k-1}, \tag{7.6}$$

for all integral values of $n \geq 0$. We are now able to show that whatever the initial conditions on (X_i), we know that $\tau(m)$ must be a divisor of $\pi(m)$.

Theorem 107 *For $\tau(m)$ and $\pi(m)$ defined as above, $\tau(m)$ divides $\pi(m)$.*

Proof Put $\pi = \pi(m)$. By (7.6) we have:

$$X_{i+\pi} = b_0 Z_{i+\pi} + b_1 Z_{i+\pi+1} + b_2 Z_{i+\pi+2} + \ldots + b_{k-1} Z_{i+\pi+k-1};$$

thus, for all sufficiently large i, we get from (7.4) that

$$X_{i+\pi} \equiv b_0 Z_i + b_1 Z_{i+1} + b_2 Z_{i+2} + \ldots + b_{k-1} Z_{i+k-1} = X_i \pmod{m}.$$

The theorem now follows easily by our previous remarks. □

We next provide a sequence of theorems concerning $\pi(p^a)$, where p is any prime. In the case where $k = 2$, we note that $Z_n = U_n(P_1, P_2)$; thus, these results can be considered as generalizations of some of the arithmetic properties of U.

Theorem 108 *For any prime p and $a \geq 1$, we have $\pi(p^{a+1}) \mid p\pi(p^a)$.*

Proof Put $\pi = \pi(p^a)$. For all sufficiently large i, we have $p^a \mid Z_{i+\pi} - Z_i$. Put $Y_i = (Z_{i+\pi} - Z_i)/p^a$ and observe that Y_i satisfies (7.2); thus, there is some $\tau = \tau(p^a)$ such that $Y_{i+\tau} \equiv Y_i \pmod{p^a}$ and $\tau \mid \pi$ by Theorem 107. Hence, $p^a Y_{i+\pi} \equiv p^a Y_i \pmod{p^{2a}}$ for sufficiently large i. Since $Z_{i+\pi} = Z_i + p^a Y_i$, we can show by induction on j that for i large enough, we have:

$$Z_{i+j\pi} \equiv Z_i + jp^a Y_i \pmod{p^{2a}}. \tag{7.7}$$

Since $2a \geq a+1$, we see that for $j = p$, we get $Z_{i+p\pi} \equiv Z_i \pmod{p^{a+1}}$ and the result follows. □

From Theorem 108, we also see that since $\pi(p^a) \mid \pi(p^{a+1})$, we must have $\pi(p^{a+1}) = \pi(p^a)$ or $\pi(p^{a+1}) = p\pi(p^a)$.

Theorem 109 *For any prime p and integer $a \geq 2$, we have $\pi(p^{a+2}) \neq \pi(p^{a+1})$ when $\pi(p^{a+1}) \neq \pi(p^a)$.*

Proof If we define (Y_i) as in the proof of Theorem 108, we see by (7.7) that we cannot have $p \mid Y_i$ for all arbitrarily large i, for otherwise we would have $\pi(p^{a+1}) \neq \pi(p^a)$. Since $2a \geq a+2$, on putting $j = p$ in (7.7), we get:

$$Z_{i+j\pi} \equiv Z_i + p^{a+1} Y_i \pmod{p^{a+2}}.$$

Since p cannot divide Y_i for some sufficiently large i, we cannot have $\pi(p^{a+2}) \neq \pi(p^{a+1})$. □

By repeatedly applying Theorem 109, we see that if $a \geq 2$ and $\pi(p^{a+1}) \neq \pi(p^a)$, then $\pi(p^{a+b}) = p^b \pi(p^a)$. Thus, we have produced a result very similar to Lucas' law of repetition.

By using the theory of finite fields, we know that if p is a prime, we can decompose $f(x)$ over $\mathbb{F}_p$ as

$$f(x) \equiv f_1(x)^{e_1} f_2(x)^{e_2} \cdots f_m(x)^{e_m} \pmod{p},$$

where $f_i(x)$ is of degree k_i and irreducible over $\mathbb{F}_p$; furthermore, we may assume that the polynomials $f_i(x)$ $(1 \leq i \leq m)$ are all distinct. Notice that

$$e_1 k_1 + e_2 k_2 + \cdots + e_m k_m = k.$$

Let $e = \max_{1 \leq i \leq m}\{e_i\}$. We have $e = 1$ when p does not divide the discriminant of $f(x)$. We also let p_i denote the k_ith power of p and put $l = \mathrm{lcm}_{1 \leq i \leq m}(p_i - 1)$.

The following result corresponds to Lucas' law of appearance.

Theorem 110 *Let p be prime such that $p \nmid P_k (= f(0))$, and define the non-negative integer κ by $p^\kappa \leq e < p^{\kappa+1}$. If $e = 1$, we have $\pi(p) \mid l$ and if $e > 1$, then $\pi(p) \mid p^{\kappa+1} l$.*

Most of the above results were known to Carmichael [4] and others were added by Engstrom [6]. Further results on this topic were obtained by Ward [12]. We have followed here the presentation in Robinson [11] and an unpublished note of Curtis Bright [3]. Because of their application to electrical engineering, in particular to the construction of linear feedback shift registers, the literature concerning linear recurrences is enormous. See, in particular, Chap. 8 of [9] for a modern treatment of this material and many references.

7.2 Impulse Sequences

On page 2 of Everest et al. [7], the sequences which we have denoted by $(Z_{i,n})$ for $i = 0, 1, \ldots, k-1$ are called *impulse sequences*. In [9] the specific sequence (Z_n) or $(Z_{k-1,n})$ is called an *impulse response sequence*. It is easy to see that if (X_n) is any sequence which satisfies (7.2), then

$$X_n = X_0 Z_{0,n} + X_1 Z_{1,n} + \cdots + X_{k-1} Z_{k-1,n}.$$

Thus, the impulse sequences form a basis for all linear recurrence sequences with characteristic polynomial $f(x)$ given by (7.3). We have already mentioned that the Lucas sequence (U_n) is the impulse sequence (Z_n) when $k = 2$. Also, using the notation of Bell [2] (see Sect. 6.3), we have $x_n = Z_{0,n}$, $y_n = Z_{1,n}$, $z_n = Z_{2,n} = Z_n$ when $k = 3$, $P_1 = P$, $P_2 = Q$ and $P_3 = R$ in (6.3). Indeed, in [5] Carmichael, who denoted Z_n (or $Z_{k-1,n}$) by G_n, mentions it as one of the two possible generalizations of the Lucas sequence (U_n).

In this section we will briefly discuss some properties of the impulse sequences that correspond to those of the Lucas sequences when $k \geq 2$. We will assume here that Δ, the discriminant of $f(x)$, is nonzero. From simple results in Sect. 10.1 of [15], we see that, like the Lucas functions, the functions $Z_{i,n}$ for $i = 0, 1, 2, \ldots, k-1$ are symmetric functions of the roots of (7.3). Also, as noted in Sect. 6.3, if ρ_i is any one of the k roots of (7.3), then we can write:

$$\rho_i^n = Z_{k-1,n}\rho_i^{k-1} + Z_{k-2,n}\rho_i^{k-2} + \cdots + Z_{0,n}. \tag{7.8}$$

We can use (7.8) to develop addition and multiplication formulas for the impulse sequences. For example, we have:

$$\begin{aligned}\rho_i^{n+m} &= Z_{k-1,n+m}\rho_i^{k-1} + Z_{k-2,n+m}\rho_i^{k-2} + \cdots + Z_{0,n+m} \\ &= (Z_{k-1,n}\rho_i^{k-1} + Z_{k-2,n}\rho_i^{k-2} + \cdots + Z_{0,n}) \times \\ &\quad (Z_{k-1,m}\rho_i^{k-1} + Z_{k-2,m}\rho_i^{k-2} + \cdots + Z_{0,m}),\end{aligned}$$

for each of the distinct k roots of (7.3). From this it is easy to see that the addition formulas are

$$Z_{h,n+m} = \sum_{i=0}^{k-1} \sum_{j=0}^{k-1} Z_{i,n} Z_{j,m} Z_{h,i+j} \quad (h = 0, 1, \ldots, k-1). \tag{7.9}$$

If we put $m = 1$ and use the values of $Z_{j,1}$ $(= \delta_{j,1})$ for $j = 0, 1, \ldots, k-1$, we get:

$$Z_{h,n+1} = \sum_{i=0}^{k-1} Z_{i,n} Z_{h,i+1}.$$

Hence, for $h = 0$ and $1 \leq h < k$, we have:

$$Z_{0,n+1} = (-1)^{k-1} P_k Z_{k-1,n};\ Z_{h,n+1} = Z_{h-1,n} + (-1)^{k-h+1} P_{k-h} Z_{k-1,n}. \tag{7.10}$$

If we put $m = n$ in (7.9), we get the doubling formulas:

$$Z_{h,2n} = \sum_{i=0}^{k-1} \sum_{j=0}^{k-1} Z_{i,n} Z_{j,n} Z_{h,i+j} \quad (h = 0, 1, \ldots, k-1), \tag{7.11}$$

and if we put $m = n + 1$ in (7.9), we get the formulas:

$$Z_{h,2n+1} = \sum_{i=0}^{k-1} \sum_{j=0}^{k-1} Z_{i,n} Z_{j,n+1} Z_{h,i+j} \quad (h = 0, 1, \ldots, k-1). \tag{7.12}$$

If we make use of (7.10) in (7.12), we can get formulas for $Z_{h,2n+1}$ for $h = 0, 1, 2, \ldots, k-1$ in terms of $Z_{i,n}$ $(i = 0, 1, 2, \ldots, k-1)$. This means that if we define the k-tuple $\mathcal{T}_h$ as $\{Z_{0,h}, Z_{1,h}, Z_{2,h}, \ldots, Z_{k-1,h}\}$, then given the k-tuple $\mathcal{T}_n$, we can compute the two k-tuples $\mathcal{T}_{2n}$ and $\mathcal{T}_{2n+1}$. Furthermore, by appealing to (7.10) and then (7.11) with n replaced by $n + 1$, we can also compute $\mathcal{T}_{2n+2}$. Each of these three k-tuples can be calculated in $O(k^2)$ multiplication and addition operations. As a consequence of this, we can then use the ideas of Sect. 3.3 to compute, given any positive integer m, the k-tuple $\mathcal{T}_m$ in $O(k^2 \log m)$ multiplication and addition operations, given only the coefficients of $f(x)$. For other approaches to the problem of computing remote terms in a linear recurrence, see the work of Miller and Spencer-Brown [10] and of Fiduccia [8].

The multiplication formulas can be derived from

$$\begin{aligned} \rho_i^{nm} &= Z_{k-1,nm} \rho_i^{k-1} + Z_{k-2,nm} \rho_i^{k-2} + \cdots + Z_{0,nm} \\ &= (Z_{k-1,n} \rho_i^{k-1} + Z_{k-2,n} \rho_i^{k-2} + \cdots + Z_{0,n})^m \end{aligned}$$

and the multinomial theorem. If we let $C(i_0, i_1, \ldots, i_{k-1})$ denote the multinomial coefficient $m!/(i_0! i_1! \cdots i_{k-1}!)$, then

$$Z_{h,nm} = \sum_{\{i_0,i_1,\ldots,i_{k-1}\}} C(i_0,i_1,\ldots,i_{k-1}) Z_{h,s} \prod_{j=0}^{k-1} (Z_{j,n})^{i_j}, \tag{7.13}$$

where the sum is taken over all the sets of nonnegative integers $\{i_0, i_1, \ldots, i_{k-1}\}$ such that $\sum_{j=0}^{k-1} i_j = m$ and $s = s(i_0, i_1, \ldots, i_{k-1}) = \sum_{j=0}^{k-1} j \cdot i_j$.

Furthermore, by observing that $\rho_0\rho_1 \cdots \rho_{k-1} = P_{k-1}$, we have:

$$P_{k-1}^n = \prod_{i=0}^{k-1} (Z_{k-1,n}\rho_i^{k-1} + Z_{k-2,n}\rho_i^{k-2} + \cdots + Z_{0,n}). \tag{7.14}$$

We next derive some arithmetic properties of the $(Z_{n,h})$ sequences. We first observe by the results in the previous section that if we put $\mathcal{Z}_n = (Z_{0,n}, Z_{1,n}, Z_{2,n}, \ldots, Z_{k-1,n})$, then for all $n \geq 0$, we have:

$$\mathcal{Z}_{n+\pi} \equiv \mathcal{Z}_n \pmod{m}, \tag{7.15}$$

where m is any positive integer such that $\gcd(m, P_k) = 1$. Put $\mathcal{W}_n = \gcd(Z_{1,n}, Z_{2,n}, \ldots, Z_{k-1,n})$; from (7.13) it is easy to see that $(\mathcal{W}_n)$ is a divisibility sequence. When $k = 3$, we get from (7.10) that

$$Z_{2,n+1} = Z_{1,n} + P_1 Z_{2,n};$$

hence, in this case $\mathcal{W}_n = \gcd(Z_{1,n}, Z_{2,n}) = \gcd(Z_{2,n+1}, Z_{2,n}) = \gcd(U_{n+1}, U_n)$, the sequence discussed in Ballot [1].

Since $\mathcal{Z}_0 = (1, 0, 0, \ldots, 0)$, we see by (7.15) that m is a divisor of $\mathcal{W}_\pi$. Call the least positive value of n such that m divides $\mathcal{W}_n$ the *rank of appearance* of m in $(\mathcal{W}_n)$ and denote it by $\omega = \omega(m)$. We now have a generalization of Theorem 8.

Theorem 111 *Suppose* $\gcd(m, P_k) = 1$. *If* ω *is the rank of appearance of* m *in* $(\mathcal{W}_i)$ *and* $m \mid \mathcal{W}_n$, *then* $\omega \mid n$.

Proof Let $n = q\omega + r$, where $0 \leq r < \omega$. By (7.9), we get

$$0 \equiv Z_{h,\,q\omega+r} = \sum_{i=0}^{k-1}\sum_{j=0}^{k-1} Z_{i,q\omega} Z_{j,r} Z_{h,i+j} \pmod{m} \quad (h = 0, 1, \ldots, k-1).$$

Since $Z_{i,q\omega} \equiv 0 \pmod{m}$ for $i > 0$, we have $0 \equiv Z_{h,\,q\omega+r} = \sum_{j=0}^{k-1} Z_{0,q\omega} Z_{j,r}$ $Z_{h,j} \equiv Z_{0,q\omega} Z_{h,r} \pmod{m}$ for $h = 1, \ldots, k-1$. By (7.14) we have $(Z_{0,q\omega})^k \equiv P_{k-1}^{q\omega} \pmod{m}$; hence, $\gcd(Z_{0,q\omega}, m) = 1$, and therefore $Z_{h,r} \equiv 0 \pmod{m}$ for $h = 1, \ldots, k-1$. Thus, $m \mid \mathcal{W}_r$. It follows that by definition of ω, we must have $r = 0$ and $\omega \mid n$. □

Corollary 112 If $\gcd(m, P_k) = 1$, then $\omega(m) \mid \pi(m)$. □

As must now be evident, many other results analogous to those involving the Lucas sequences can be derived for the impulse sequences. It is remarkable, given Lucas' interest in linear recurrence sequences, that he did not investigate these impulse sequences further. Perhaps he intended to do so, but no evidence of this seems to have survived. We will discuss this at greater length later in the next chapter, but for now we will turn our attention to generalizing the Lehmer sequences.

7.3 A Return to the Lehmer Sequences

In order to generalize the Lehmer sequences in Sect. 4.4, it is helpful to define the four sequences $(V_{i,n})$ and $(U_{i,n})$ for $i = 0, 1$. Here we put:

$$\begin{cases} V_{0,n} = \overline{V}_n(R,Q) \text{ and } V_{1,n} = 0; \quad U_{0,n} = 0 \text{ and } U_{1,n} = \overline{U}_n(R,Q), \\ \text{if } n \text{ is even;} \\ V_{0,n} = 0 \text{ and } V_{1,n} = \overline{V}_n(R,Q); \quad U_{0,n} = \overline{U}_n(R,Q) \text{ and } U_{1,n} = 0, \\ \text{if } n \text{ is odd.} \end{cases}$$

Let ρ_1, ρ_2 be the roots of $x^2 - R$ and let $\alpha_i + \beta_i = \rho_i$ and $\alpha_i\beta_i = Q$ $(i = 1, 2)$; notice that since $\rho_1 = -\rho_2$, we get $\alpha_1 = -\alpha_2$ or $\beta_1 = -\beta_2$. It is not difficult to see, then, that

$$\frac{\alpha_i^n - \beta_i^n}{\alpha_i - \beta_i} = U_{0,n} + \rho_i U_{1,n}, \quad \alpha_i^n + \beta_i^n = V_{0,n} + \rho_i V_{1,n} \quad (i = 1, 2). \tag{7.16}$$

We can use (7.16) as an indication of how to extend the Lehmer sequences. As in Sect. 7.2, we let $\rho_1, \rho_2, \ldots, \rho_k$ be the roots of $f(x)$, where $f(x)$ is given by (7.3), and we assume that Δ, the discriminant of $f(x)$, is not zero. For a given nonzero integer Q, we define α_i, β_i by $\alpha_i + \beta_i = \rho_i$ and $\alpha_i\beta_i = Q$ $(i = 1, 2, \ldots, k)$. By analogy to (7.16), we now define the $2k$ functions $U_{i,n}$ and $V_{i,n}$ $(i = 0, 1, 2, \ldots, k-1)$ by

$$\frac{\alpha_i^n - \beta_i^n}{\alpha_i - \beta_i} = U_{0,n} + \rho_i U_{1,n} + \rho_i^2 U_{2,n} + \cdots + \rho_i^{k-1} U_{k-1,n}, \tag{7.17}$$

and

$$\alpha_i^n + \beta_i^n = V_{0,n} + \rho_i V_{1,n} + \rho_i^2 V_{2,n} + \cdots + \rho_i^{k-1} V_{k-1,n}. \tag{7.18}$$

Since the roots of $f(x)$ are all distinct $(\Delta \neq 0)$, we see immediately that

$$U_{i,0} = 0, \; V_{i,0} = 2\delta_{i,0}, \; U_{i,1} = \delta_{i+1,1}, \; V_{i,1} = \delta_{i,1} \quad (i = 0, 1, \ldots, k-1);$$

furthermore, since the identities (2.35) and (2.36) hold for any pairs (P, Q), even when P is not an integer, and

$$\frac{\alpha_i^n - \beta_i^n}{\alpha_i - \beta_i} = U_n(\rho_i, Q), \quad \alpha_i^n + \beta_i^n = V_n(\rho_i, Q), \tag{7.19}$$

we see that $U_{i,n}$ and $V_{i,n}$ are all integers for $n \geq 0$ and $i = 0, 1, \ldots, k-1$.

If we set $h_i(x) = x^2 - \rho_i x + Q$, then

$$F(x) = h_1(x)h_2(x)\ldots h_k(x) = x^k f(x + Q/x)$$

is a polynomial of degree $2k$ with integer coefficients whose roots are α_i, β_i $(i = 0, 1, \ldots, k-1)$. Indeed, if we put

$$F(x) = x^{2k} - R_1 x^{2k-1} + R_2 x^{2k-2} - \cdots + R_{2k},$$

then $(U_{i,n})$ and $(V_{i,n})$ both satisfy the linear recurrence:

$$X_{n+2k} = R_1 X_{n+2k-1} - R_2 X_{n+2k-2} + \ldots - R_{2k} X_n. \tag{7.20}$$

For example, when $k = 2$, we have $R_1 = P_1$, $R_2 = P_2 + 2Q$, $R_3 = QP_1$, $R_4 = Q_2$ and when $k = 3$ we have $R_1 = P_1$, $R_2 = P_2 + 3Q$, $R_3 = P_3 + 2P_1Q$, $R_4 = QR_2$, $R_5 = Q^2R_1$, $R_6 = Q^3$.

Also, as shown in Sect. 10.1 of [15], the discriminant D of $F(x)$ can be evaluated as

$$D = E\Delta^2 Q^{k(k-1)}, \tag{7.21}$$

where E is the integer $f(2\sqrt{Q})f(-2\sqrt{Q}) = (\rho_1^2 - 4Q)(\rho_2^2 - 4Q)\ldots(\rho_k^2 - 4Q) = \prod_{i=1}^{k}(\alpha_i - \beta_i)^2$. In the case of $k = 2$, we get $E = (P_2 + 4Q)^2 - 4QP_1^2$.

If $k = 1$, we have $U_{0,n} = U_n(P_1, Q)$ and $V_{0,n} = V_n(P_1, Q)$, and we have already seen that when $k = 2$, $P_1 = 0$, $P_2 = R$, we get Lehmer's sequences from $(U_{i,n})$ and $(V_{i,n})$, as described above. In [14] (see also Chap. 10 of [11]), Williams showed that these *generalized Lehmer sequences* have many of the features possessed by the Lucas sequences. Given the definition of $(U_{i,n})$ and $(V_{i,n})$ and (7.19), it is not surprising that we can derive several identities involving these sequences; indeed, there are addition formulas, multiplication formulas, and techniques for computing remote values of terms of these sequences. In particular, we mention that when computing faraway terms of these sequences modulo some N such that $\gcd(N, Q) = 1$, it is somewhat more convenient to work with the $(V_{i,n})$ sequences rather than the $(U_{i,n})$ sequences. We do this by analogy to the Lucas sequence case by defining $W_{i,n} \equiv Q^{-n}V_{i,2n} \pmod{N}$ $(i = 0, 1, 2, \ldots, k-1)$ and working with the $(W_{i,n})$ sequences modulo N. From (10.2.5) of [15], we can produce the addition formula:

$$W_{m+n} \equiv \sum_{i=0}^{k-1} \Big(\sum_{j=0}^{k-1} W_{i,n} W_{j,n} Z_{h,i+j} \Big) - W_{h,n-m} \pmod{N},$$

where the sequences $(Z_{i,n})$ for $i = 0, 1, \ldots, k-1$ are the impulse sequences with characteristic polynomial $f(x)$. We also have the initial values:

$$W_{i,0} \equiv 2\delta_{i,0}, \quad QW_{i,1} \equiv Z_{i,2} - 2Q\delta_{i,0} \pmod{N} \quad (i = 0, 1, \ldots, k-1).$$

If for any positive integer j, we define the k-tuple $\mathcal{W}_j$ to be

$$\{W_{0,j}, W_{1,j}, \ldots, W_{k-1,j}\},$$

we see that, given any pair of these k-tuples $\mathcal{W}_n$ and $\mathcal{W}_{n+1}$ modulo N, the formulas (10.2.15) and (10.2.16) of [15] can be used to compute $\mathcal{W}_{2n}$, $\mathcal{W}_{2n+1}$, and $\mathcal{W}_{2n+2} \pmod{N}$ in $O(k^2)$ addition and modular multiplication operations. It follows that the ideas of Sect. 3.3 can then be used to compute the remote k-tuple $\mathcal{W}_t \pmod{N}$ in $O(k^2 \log t)$ modular multiplication and addition operations modulo N.

It needn't be the case that any of $(U_{i,n})$ or $(V_{i,n})$, $i = 0, 1, \ldots, k-1$, is a divisibility sequence, but if we put $\mathcal{A}_n = \gcd(U_{0,n}, U_{1,n}, \ldots, U_{k-1,n})$ and, when $k > 1$, $\mathcal{C}_n = \gcd(V_{1,n}, V_{2,n}, \ldots, V_{k-1,n})$, then both $\mathcal{A}_n$ and $\mathcal{C}_n$ are divisibility sequences. Furthermore, if m is a positive integer such that $\gcd(m, Q) = 1$, the sequence $(\mathcal{A}_n)$ has a rank of appearance modulo m, which we will denote here by $\omega = \omega(m)$. In [15] it is shown that if $m \mid \mathcal{A}_n$ for some $n \geq 0$, then $\omega \mid n$. It is possible to develop laws of repetition and appearance for the generalized Lehmer sequences; it is even possible to extend Lucas' Fundamental theorem to these sequences and to develop primality tests analogous to those of Lucas. All of this is described in some detail in Chaps. 10–12 of [15].

7.4 Primality

As we have seen, Lucas was motivated in his search for generalizations of his sequences because of his belief that they might provide a means of discovering new properties of prime numbers. In particular, he was interested in primality testing, and we know he was attracted to the problem of proving the primality of numbers of the form

$$N = Ap^n + \gamma, \tag{7.22}$$

where p is an odd prime, $2 \mid A$, $p \nmid A$, $\gamma \in \{1, -1\}$, and $A < p^n$. Thus, it seems appropriate here to examine the problem of proving N a prime by using the generalized Lehmer sequences.

Let $s = (p-1)/2$ and q be any prime such that $q \equiv 1 \pmod{p}$, $q \nmid N$ and $N^{(q-1)/p} \not\equiv 1 \pmod{q}$. By Theorem 11.3.6 of [15], we see that a necessary and sufficient test for the primality of N, involving the Lucas sequences and similar to the $p = 3$ case of Theorem 56, can be derived when we have a priori some integer R such that $G_s(R) \equiv 0 \pmod{N}$. Indeed, if we can find any

Lucas sequence (U_n) such that $(D \mid N) = \gamma$ and $N \nmid U_A$, then it is an easy matter to find some R such that either $N \mid G_s(R)$ or N is not a prime. For most values of N, such a Lucas sequence is easy to find, but in some cases this problem can be difficult. In what follows we will show how the generalized Lehmer sequences can be used in the development of necessary and sufficient tests for the primality of numbers N, given by (7.22), which dispense entirely with the need to find R. We stress here that these tests are only of theoretic interest, as the use of a result like Theorem 54 or Theorem 57 is almost always adequate to establish the primality of N.

In Sect. 11.1 of [15], it is shown how to compute s integers $P(i,p,q)$ $(i = 1, 2, \ldots, s)$ such that if we put $k = s$ and $P_i = P(i,p,q)$ in (7.3), the corresponding sequences $(\mathcal{A}_n)$, $(\mathcal{C}_n)$ associated with the generalized Lehmer sequences for this particular $f(x)$ with $Q = q^{p-2}$ have some special properties. In order to discuss these, we first need to define the function $\theta(m)$.

Let m be any odd positive integer such that $p \nmid m$. If we let ν $(= \nu(m))$ be the index to which m belongs modulo p, we define $\theta(m) = (m^\mu + (-1)^\nu)/p$, where $\mu = \nu$ when ν is odd and $\mu = \nu/2$, otherwise. Notice that since $\nu \mid p-1$, we have $2p\theta(m) \mid m^{p-1} - 1$. The following is a very slight modification of Theorem 11.2.3 in [15].

Theorem 113 *Let the sequences $(\mathcal{A}_n)$ and $(\mathcal{C}_n)$ be those obtained from the generalized Lehmer sequences with $k = s$, $P_i = P(i,p,q)$ $(i = 1, 2, \ldots, s)$ and $Q = q^{p-2}$. Suppose r $(\neq p)$ is any prime such that $r \nmid q\Delta$ and put $\theta = \theta(r)$. If $r^{(q-1)/p} \equiv 1 \pmod q$, then $r \mid A_\theta$ and $r \mid C_\theta$; if $r^{(q-1)/p} \not\equiv 1 \pmod q$, then $r \mid \mathcal{A}_{p\theta}$ and $r \mid \mathcal{C}_{p\theta}$, but $r \nmid \mathcal{A}_{n\theta}\mathcal{C}_{n\theta}$ when $p \nmid n$.*

(We have replaced $D(F)$ or D by Δ in this version, but if we refer to the proof of Theorem 10.4.4 in [15], we see that the result is certainly true when $|\epsilon_i| = 1$ for all $i \leq \lambda$. However, it is shown in the proof of case 1 of Theorem 10.3.10 that $\epsilon_j = -1$, 0 or 1; if $\epsilon_j = 0$, we have $p \mid r$, which is impossible. Thus, by (7.21) we can replace D by $q\Delta$.)

If we let N be of the form (7.22), we can obtain a somewhat more general version of Theorem 11.2.6 of [15] when $(\mathcal{A}_n)$ is defined as in Theorem 113.

Theorem 114 *Let N be of the form (7.22) and let $(\mathcal{A}_n)$ be defined as in Theorem 113. Put $\theta = \theta(N) = N - \gamma = Ap^n$. If $\gcd(N, pq\Delta) = 1$, $N \mid \mathcal{A}_{p\theta}$, and $N \nmid \mathcal{A}_\theta$, then there must exist a prime divisor r of N such that*

$$r^{p-1} \equiv 1 \pmod{p^n}.$$

Proof If $N \mid \mathcal{A}_{p\theta}$ and $N \nmid \mathcal{A}_\theta$, there must exist a prime divisor r of N such that $r^b \,||\, N$ $(b \geq 1)$ and $r^b \nmid \mathcal{A}_\theta$. It follows that $\omega(r^b) \mid p\theta$ and $\omega(r^b) \nmid \theta$; hence, $p^n \mid \omega(r^b)$. By the law of repetition for $(\mathcal{A}_n)$ (Theorem 10.3.17 of [15]), we know that $\omega(r^b) \mid r^m\omega(r)$ for some $m \geq 0$. Thus, we get $p^n \mid \omega(r)$ and therefore $p^n \mid p\theta(r)$ by Theorem 113. It follows from the definition of $\theta(r)$ that

$$r^{p-1} \equiv 1 \pmod{p^n}. \qquad \square$$

By appealing to results in Sect. 10.4 of [15], it is also possible to prove the following theorem.

Theorem 115 *Let N be of the form (7.22) and let $(\mathcal{C}_n)$ be defined as in Theorem 113. Put $\theta = \theta(N) = N - \gamma = Ap^n$. If $\gcd(N, pq\Delta) = 1$, $N \mid \mathcal{C}_{p\theta}$, and $N \nmid \mathcal{C}_{p\theta}$, then there must exist a prime divisor r of N such that*

$$r^{p-1} \equiv 1 \pmod{p^n}.$$

These results lead us to a study of the congruence

$$x^{p-1} \equiv 1 \pmod{p^m} \tag{7.23}$$

for a given prime p and positive integer m. Let h be any primitive root of p. Define $g_1(p,m) \equiv h^{p(m)} \pmod{p^m}$, where $p(m) = p^{m-1}$ and put $g_i(p,m) \equiv g_1(p,m)^i \pmod{p^m}$, for $i = 1, 2, \ldots, p-1$. Since $(p-1)p(m) = \varphi(p^m)$, we observe that $g_i(p,m)^{p-1} \equiv 1 \pmod{p^m}$; also, if $g_i(p,m) \equiv g_j(p,m) \pmod{p^m}$ for $1 \le i, j \le p-1$, then $h^{(j-i)p(m)} \equiv 1 \pmod{p^m}$, which means that $p-1$ must divide $i-j$; given the range of i and j, we can only have $i = j$. Thus, $g_i(p,m)$ for $i = 1, 2, \ldots, p-1$ are the $p-1$ distinct roots of (7.23). Furthermore, $g_{p-1}(p,m) \equiv 1 \pmod{p^m}$; thus, if $N > p^n$ and $g_i(p,n) \mid N$ for some i such that $1 \le i < p-1$, then N must be composite.

We may assume with no loss of generality that $0 < g_i(p,m) < p^m$ for $i = 1, 2, \ldots, p-1$. We also notice that both $g_i(p,m)$ and $p^m - g_i(p,m)$ are distinct roots of (7.23); hence, there are exactly s values of the $g_i(p,m)$ $(i = 1, 2, \ldots, p-1)$ which are odd. Thus, if N satisfies the conditions of Theorem 114, there exists a prime divisor r of N such that $r = g_i(p,n) + tp^n$ for some $t \ge 0$ and some i such that $1 \le i \le p-1$. We next prove a result similar to Lemma 20.

Lemma 33 *Suppose that N is given by (7.22), where $n \ge 1$ and $g_i(p,n) \nmid N$ for any i such that $g_i(p,n)$ is odd and $1 \le i < p-1$. If N has at least one prime divisor r of the form $r = g_i(p,n) + tp^n$ for some $t \ge 0$ and some i such that $1 \le i \le p-1$, then N is a prime.*

Proof We proceed as in the proof of Lemma 20. Suppose N is composite and write $N = rT$, where $T > 1$. We get $rT \equiv \gamma \pmod{p^n}$ and therefore $g_i(p,n)T \equiv \gamma \pmod{p^n}$. Since

$$1 = \gamma^{p-1} \equiv (g_i(p,n)T)^{p-1} \equiv T^{p-1} \pmod{p^n},$$

we must have $T \equiv g_j(p,n) \pmod{p^n}$ for some j such that $1 \le j \le p-1$. Hence, $T = vp^n + g_j(p,n)$, where $v \ge 0$. By the conditions of the theorem, we must have $t, v \ge 1$; however, this means that $N > p^{2n}$, which contradicts $A < p^n$. □

We can now combine the results of Theorem 114 and Lemma 33 to obtain a necessary and sufficient test for the primality of N given by (7.22).

Theorem 116 *Suppose that N is given by (7.22), where $n \geq 1$ and* $\gcd(N, q\Delta) = 1$. *Suppose further that $N^{(q-1/p)} \not\equiv 1 \pmod{q}$ and that $g_i(p,n) \nmid N$ for any i such that $g_i(p,n)$ is odd and $1 \leq i < p-1$. If $(\mathcal{A}_n)$ is defined as in Theorem 113 and $m = (N-\gamma)/p$, then N is a prime if and only if $N \mid \mathcal{A}_{pm}$, and $N \nmid \mathcal{A}_m$.*

Proof If N is a prime, then $N \mid \mathcal{A}_{pm}$, and $N \nmid \mathcal{A}_m$ by Theorem 113. If $N \mid \mathcal{A}_{pm}$, and $N \nmid \mathcal{A}_m$, then N must be a prime by Theorem 114 and Lemma 33. □

We remark here that we can use Theorem 113, Theorem 115, and Lemma 33 to prove a result analogous to Theorem 116 for the $(\mathcal{C}_n)$ sequence.

Theorem 117 *Suppose that N is given by (7.22), where $n \geq 1$ and* $\gcd(N, q\Delta) = 1$. *Suppose further that $N^{(q-1)/p} \not\equiv 1 \pmod{q}$ and that $g_i(p,n) \nmid N$ for any i such that $g_i(p,n)$ is odd and $1 \leq i < p-1$. If $(\mathcal{C}_n)$ is defined as in Theorem 113 and $m = (N-\gamma)/p$, then N is a prime if and only if $N \mid \mathcal{C}_{pm}$, and $N \nmid \mathcal{C}_m$.*

Theorem 116 is a necessary and sufficient analogue, using the sequence $(\mathcal{A}_n)$ instead of (U_n), of the test given as Theorem 54. It is even possible to produce a test, involving the $(W_{i,n})$ sequence modulo N, which is a necessary and sufficient version of the test given as Theorem 57.

Theorem 118 *Suppose N is given by (7.22), where $n \geq 1$ and* $\gcd(N, q\Delta) = 1$. *Suppose further that $N^{(q-1)/p} \not\equiv 1 \pmod{q}$ and that $g_i(p,n) \nmid N$ for any i such that $g_i(p,n)$ is odd and $1 \leq i < p-1$. If $m = (N-\gamma)/p$, then N is prime if and only if*

$$Y_{i,s}(W_{0,m}, W_{1,m}, \ldots, W_{s-1,m}) \equiv 0 \pmod{N} \quad (i = 0, 1, \ldots, s-1).$$

Here the $Y_{i,n}(x_0, x_1, \ldots, x_{k-1})$ $(i = 0, 1, \ldots, k-1)$ are k polynomials, each in k variables and of degree n, defined by

$$G_n(x_0 + x_1\rho + x_2\rho^2 + \ldots + x_{k-1}\rho^{k-1}) = Y_{0,n} + Y_{1,n}\rho + Y_{2,n}\rho^2 + \ldots + Y_{k-1,n}\rho^{k-1}$$

for all the roots of $f(x)$. For example, $Y_{i,0}(x_0, x_1, \ldots, x_{k-1}) = \delta_{i,0}$, $Y_{i,1}(x_0, x_1, \ldots, x_{k-1}) = x_i + \delta_{i,0}$. Also, if $k = n = 1$, we have the single polynomial $Y_{0,1} = x_0 + 1$; if $k = n = 2$, we have the two polynomials $Y_{0,2}(x_0, x_1) = x_0^2 - P_2 x_1^2 + x_0 - 1$, $Y_{1,2}(x_0, x_1) = P_1 x_1^2 + 2x_0 x_1 + x_1$. Notice that

$$\begin{aligned} Y_{1,2}(x_0, x_1) &= x_1(P_1 x_1 + 2x_0 + 1), \\ 4Y_{0,2}(x_0, x_1) &= (P_1 x_1 + 2x_0 + 1)^2 - 2P_1 x_1(P_1 x_1 + 2x_0 + 1) + \Delta x_1^2 - 5. \end{aligned} \tag{7.24}$$

In general, for any fixed $n \geq 1$, we can compute $Y_{i,n} = Y_{i,n}(x_0, x_1, \ldots, x_{k-1})$ $(i = 0, 1, \ldots, k-1)$ recursively by making use of the formula:

$$Y_{h,l+1} = \sum_{i=0}^{k-1} \sum_{j=0}^{k-1} x_j Y_{i,l} Z_{h,i+j} - Y_{h,l-1}.$$

This formula can be easily derived from the identity $G_{l+1}(x) = xG_l(x) - G_{l-1}(x)$ and (7.8). The $(Z_{h,i})$ sequences here are, as in the previous section, the impulse sequences with characteristic polynomial $f(x)$. When n is large, more efficient methods of computing $Y_{i,n}$ $(i = 0, 1, \ldots, k-1)$ can be deduced from (4.18).

There are many other methods for computing the $Y_{i,s}(W_{0,m}, \ldots, W_{s-1,m})$ in Theorem 118; for example, another technique can be derived as follows. For any integer $n \geq 0$, we simply put $W_{i,n} = V_{i,2n}/Q^n$ $(i = 0, 1, 2, \ldots, k-1)$ and define

$$X_{i,n} = \sum_{h=0}^{s-1} W_{h,n} \rho_i^n; \tag{7.25}$$

by (7.18) and the second formula of (7.19) we see that we can write $X_{i,n} = C_{2n}(\rho_i/\sqrt{Q})$ for the $C_n(x)$ defined by (4.7). By (4.13) we get:

$$C_j(X_{i,n}) = C_{2jn}(\rho_i/\sqrt{Q}) = \sum_{h=0}^{s-1} W_{h,jn} \rho_i^h. \tag{7.26}$$

From (4.7) and (7.25), we find that

$$G_s(X_{i,n}) = \sum_{j=1}^{s} C_j(X_{i,n}) + 1 = \sum_{j=1}^{s} \Big(\sum_{h=0}^{s-1} W_{h,jn} \rho_i^h \Big) + 1.$$

It follows from the definition of the $Y_{i,s}$ $(i = 0, 1, \ldots, s-1)$ that we have

$$Y_{i,s}(W_{0,m}, W_{1,m}, \ldots, W_{s-1,m}) \equiv \sum_{j=1}^{s} W_{i,jm} + \delta_{i,0} \pmod{N}.$$

We see here that Theorem 118 is a generalization for any odd p of Theorem 56; for, in the case of $p = 3$ we have $s = 1$, $m = (N-\gamma)/3$, $Y_{0,1}(W_{0,m}) = W_{0,m}+1$, $W_{0,m} \equiv Q^{-m} V_{0,2m} \pmod{N}$, and $V_{0,2m} = V_{2m}(P_1, Q)$, where $Q = q$ and $P_1 = P(1, 3, q) = t$. For the case of $p = 5$ $(i = 0, 1, \ldots, k-1)$, we have $s = 2$. Put $P_i = P(i, 5, q)$ $(i = 1, 2)$ and $Q = q^3$, where q $(\equiv 1 \pmod 5)$ and r are primes such that $\gcd(r, 5q\Delta) = 1$ and $r^{(q-1)/5} \not\equiv 1 \pmod q$. By Theorem 113 we cannot have $r \mid W_{i,m}$ for $m = (N-\gamma)/5$. Thus, in view of (7.24), a $p = 5$ version of Theorem 56 can be given as follows.

Theorem 119 *Suppose that N is given by (7.22), where $n \geq 1$, $p = 5$ and $\gcd(N, q\Delta) = 1$. Suppose further that $N^{(q-1)/5} \not\equiv 1 \pmod q$ and that $g_i(5, n) \nmid N$ for any i such that $g_i(5, n)$ is odd and $1 \leq i \leq 3$. If $m = (N-\gamma)/5$, then N is a prime if and only if*

$$2W_{0,m} + P_1 W_{1,m} \equiv -1 \pmod{N} \quad \textit{and} \quad \Delta W_{1,m}^2 \equiv 5 \pmod{N}.$$

We conclude this section by emphasizing that, just as in the case of Theorem 53, these results, as tests for primality, are not effective in that they do not completely specify for any given N how to find a suitable value of q. This obstruction is discussed at some length in Sect. 16.4 of [15], and it seems that in most cases it is not a difficult problem, in practice, to find an appropriate q for most values of N. Certainly, we can easily specify an infinitude of possible values of N for which it is easy to find a satisfactory value for q.

References

1. C. Ballot, *A weak generalization of ordinary Lucas sequences involving the sequence* $\{A^N + B^N + C^N\}_{N\geq 0}$, Congr. Numer. **194** (2009), 39–44.
2. E. T. Bell, *Notes on recurring series of third order*, Tohoku Math. J. **24** (1924),168–184.
3. C. Bright, *Modular Periodicity of Linear Recurrence Sequences*, unpublished. See https://cs.uwaterloo.ca/~cbright/reports/PM434Project.pdf
4. R. D. Carmichael, *On sequences of integers defined by a recurrence relation*, Quart. J. Math. **48** (1920), 343–372.
5. R. D. Carmichael, *A simple principle of unification in the elementary theory of numbers*, Amer. Math. Monthly **36** (1929), 132–143.
6. H. T. Engstrom, *On sequences defined by linear recurrence relations*, Trans. Amer. Math. Soc. **33** (1931), 210–218.
7. Graham Everest, Alf van der Poorten, Igor Shparlinski, Thomas Ward, *Recurrence Sequences*, Mathematical Surveys and Monographs **104**, AMS, Providence RI, 2003.
8. C. M. Fiduccia, *An efficient formula for linear recurrences*, SIAM J. Comp. **14.1** (1985), 106–112.
9. Rudolph Lidl and Harald Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983.
10. J. C. P. Miller and D. J. Spencer-Brown, *An algorithm for evaluation of remote terms in a linear recurrence sequence*, Computer Journal **9** (1966-67), 188–190.
11. D. W. Robinson, *A note on linear recurrent sequences*, Amer. Math. Monthly **73** (1966), 619–621.
12. M. Ward, *The arithmetical theory of linear recurring series*, Trans. Amer. Math. Soc. **35** (1933), 600-618.
13. M. Ward, *The null divisors of linear recurring series*, Duke Math. J. **2** (1936), 472–476.
14. H. C. Williams, *A generalization of Lehmer's functions*, Acta Arith. **29** (1976), 315–341.
15. H. C. Williams, *Édouard Lucas and primality testing*, Wiley, Canadian Math. Soc. Series of Monographs and Advanced Texts, 1998.

Chapter 8
Divisibility Sequences and Further Generalizations

I do not know what I may appear to the world, but to myself I seem to have been only like a boy playing on the seashore, and diverting myself in now and then finding a smoother pebble or a prettier shell than ordinary, whilst the great ocean of truth lay all undiscovered before me. (Isaac Newton)

Abstract In this chapter we consider, starting with some early observations of Lucas, the problem of generalizing the Lucas sequences (U_n) and (V_n), by making use of certain divisibility sequences. We provide a brief discussion of Ward's elliptic divisibility sequence and its remarkable attributes. This is followed by a discussion of the properties of divisibility sequences which satisfy linear recurrences. We use these observations and the basic properties of the Lucas sequences to derive some extended Lucas sequences and list their properties in certain special cases. These sequences have features very much in common with those of (U_n) and (V_n). Finally, we discuss odd and even extensions of the Lucas sequences.

8.1 Another Suggestion of Lucas for Generalizing His Sequences

As stated in Sect. 6.1, Lucas mentioned three possible directions that might be followed in generalizing his functions. We have already examined one of these and an instance of another (Roettger's sequences). In this section and the next, we will discuss his third proposal. Later, in the following sections, we will provide a more general discussion of sequences like those given by (6.1).

In Sect. IX of [16], Lucas states:

We will complete this section with the proof of formulas of extreme importance, because these will serve later as a basis for the theory of the numerical

© Springer Nature Switzerland AG 2023

C. J.-C. Ballot, H. C. Williams, *The Lucas Sequences*, CMS/CAIMS Books in Mathematics 8, https://doi.org/10.1007/978-3-031-37238-4_8

functions of double period, derived from the consideration of the symmetric functions of the roots of the third and fourth degree with rational coefficients.

It is not exactly clear what Lucas meant by "numerical functions of double period," because the most obvious meaning would be a function F such that $F : \mathbb{Z} \to \mathbb{Z}$ and for any fixed m, we have $F(n + p_1) \equiv F(n) \pmod{m}$ and $F(n + p_2) \equiv F(n) \pmod{m}$ for all sufficiently large n and fixed (but dependent on m) integral periods p_1 and p_2. However, it is easy to see that because there exist integers x and y such that $p = xp_1 + yp_2$, then F is simply numerically periodic modulo m for the period p where $p = \gcd(p_1, p_2)$.

Lucas goes on to show that

$$U_n^2 U_{m-1} U_{m+1} - U_m^2 U_{n-1} U_{n+1} = Q^{n-1} U_{m-n} U_{m+n} \tag{8.1}$$

and

$$V_n^2 V_{m-1} V_{m+1} - V_m^2 V_{n-1} V_{n+1} = -D^2 Q^{n-1} U_{m-n} U_{m+n}. \tag{8.2}$$

Actually, he gave an incorrect version of (8.2) which was later corrected by Bell [4]. On putting $m = n + 1$ and $m = n + 2$, in (8.1), he produced the two formulas:

$$\begin{aligned} &U_n^3 U_{n+2} - U_{n+1}^3 U_{n-1} = Q^{n-1} U_1 U_{2n+1}, \quad \text{and} \\ &U_n^2 U_{n+1} U_{n+3} - U_{n+2}^2 U_{n-1} U_{n+1} = Q^{n-1} U_2 U_{2n+2}. \end{aligned} \tag{8.3}$$

He then states:

The formulas [(8.1)] and [(8.3)] belong to the theory of elliptic functions and more especially to the functions which Jacobi denoted by the symbols Θ and H. (In Lucas [17], he added the functions Θ_1 and H_1 to this remark.)

It seems, then, that Lucas, having observed the connection between his linear recurrence sequences (of degree 2) (U_n) and (V_n) to the singly periodic circular functions (see Sect. 4.1), was attempting to extend these sequences by appealing to a possible connection between some (unspecified) recurrence sequences (of order 3 or 4?) and doubly periodic elliptic functions. This was all he seems to have written concerning this idea until the remarks in his 1891 circular, quoted in Sect. 6.1.

These remarks provide us with some idea of where Lucas intended to go, but as they were published in the year of his death, he was unable to do anything further. The reference to Moutard is particularly revealing because Moutard, in investigating the Poncelet polygons, developed some results concerning a certain function A_n, which satisfies

$$A_{m-n} A_{m+n} = A_n^2 A_{m-1} A_{m+1} - A_m^2 A_{n-1} A_{n+1}, \tag{8.4}$$

the same equation (with $Q = 1$) as that satisfied by U_n in (8.1). Furthermore, if we are given values for a, b, c and $A_0 = 0$, $A_1 = 1$, $A_2 = 2abc$, $A_3 = a_2 b_2 + b_2 c_2 + a_2 c_2$, $A_4 = 4abc a_2 b_2 c_2$, where $a_2 = a^2 b^2 - b^2 c^2 + a^2 c^2$, $b_2 =$

$a^2b^2 + b^2c^2 - a^2c^2$, $c_2 = -a^2b^2 + b^2c^2 + a^2c^2$, then Moutard's A_n possesses the following features:

- A_n is a symmetric polynomial in a, b, c, of degree $n^2 - 1$, over the integers;
- (A_n) seems to be a divisibility sequence when a, b, c are the roots of a cubic polynomial with integer coefficients (Moutard did not actually prove that (A_n) is a divisibility sequence, but provided some results that strongly suggest this.);
- A_n is related to the Jacobi H function;
- If $a = b$, then $A_n = Q^{n(n-1)/2}U_n(P, Q)$, when $P = 2c$, $Q = b^2$.

Given these observations, it is easy to see how Lucas might have written the above comments. For more concerning this, see Sect. 17.4 of [35], where it is explained why Lucas might have thought that there could be solutions of (8.4) which were also linear recurrence sequences of order three or four.

8.2 Elliptic Divisibility Sequences

Although Lucas seems to have conceived the idea explained in the previous section as early as the mid to late 1870s, he appeared to make no progress on it beyond what is reported above. The next individual to try to find a connection between symmetric functions of the roots of a polynomial, through the intermediary of elliptic functions, to Lucas' sequences was E.T. Bell in [4]. Bell succeeded in clarifying some of Lucas' ideas, particularly those concerning elliptic functions, but was unable to make any substantial further progress, and as we have pointed out in Sect. 7.3 seems to have been rather pessimistic about any future advancement. Indeed, in March 23, 1930, in response to a letter written by Duncan Harkin, he [5] wrote:

> ... you ask about a feasible generalization through Elliptic Functions of the Functions of Lucas. If I knew how to do this, I [s]hould be far from telling you, as I have tried my darndest to make some real progress on it myself for the past twentyeight [*sic*] years. It is a tough nut of the first order. Whoever cracks it will make a contribution to the theory of numbers on a par with anything Fermat did. Go to it!

It was Bell's Ph. D. student, Morgan Ward, who made enormous progress on this problem. Although Ward's 1928 Ph. D. dissertation, entitled Foundations of General Arithmetic, is mainly a work on formal logic, it seems that he must have discussed Lucas' work with Bell because much of Ward's subsequent work seems to have been motivated by the problem of generalizing Lucas' sequences. For a brief summary of Ward's mathematical work, see the paper of Lehmer [14].

Ward's most important contribution to the Lucas problem was his memoir [34], which he published in the same journal in which Lucas published his memoir. In this work, he began with the recursion formula:

$$W_{m-n}W_{m+n} = W_n^2 W_{m-1}W_{m+1} - W_m^2 W_{n-1}W_{n+1}, \tag{8.5}$$

which is essentially the formula that Lucas regarded as being so important. Indeed, we observe that if $W_n = Q^{n(n-1)/2}U_n(P,Q)$, then by (8.1) (W_n) satisfies (8.5). Somewhat later in [34] Ward pointed out that if $Y_n = c^{r(n)}W_n$, where c is any nonzero constant and $r(n) = n^2 - 1$, then the sequence (Y_n) also satisfies (8.5); he called these sequences (W_n) and (Y_n) equivalent. He derived a number of important results concerning sequences satisfying (8.5) and supplemented this work with further deductions in [34]. Notice that if we put $n = m$ and assume that $W_{2n} \neq 0$ for some n, we see that $W_0 = 0$; also, if we put $n = 1$, we get $W_1 = \pm 1$. Ward confined his discussion of the solutions of (8.5) to those with initial conditions $W_0 = 0$ and the normalized $W_1 = 1$. On putting $m = n+1$ and $m = n+2$, in (8.5), it is easy to see by induction that (W_n) is completely determined, once values have been selected for W_2, W_3, W_4.

In what follows we summarize some of Ward's findings:

- The only sequences (W_n) satisfying (8.5) that are of arithmetic interest are those for which $W_0 = 0$, $W_1 = 1$ and $W_2W_3 \neq 0$. Such (W_n) are said to be *nondegenerate*.
- The sequence (W_n) is a divisibility sequence (called an *elliptic divisibility sequence* or *EDS*) if and only if W_2, W_3, W_4 are integers and $W_2 \mid W_4$.
- If (W_n) is an EDS and p is any prime, then p must divide some W_r $(r > 0)$.
- If the prime p divides W_ρ, $(\rho > 1)$ in an EDS (W_n), but $p \nmid W_r$ for any aliquot divisor r of ρ, call ρ a rank of appearance of p in (W_n). If $p \nmid \gcd(W_3, W_4)$, then $\rho \leq 2p + 1$.
- If ρ is the least rank of appearance of a prime p in (W_n) and $p \nmid W_{\rho+1}$, then $p \mid W_n$ if and only if $\rho \mid n$.
- If ρ is the least rank of appearance of a prime p in (W_n) and $p \mid W_{\rho+1}$, then $\rho \leq 3$ and $p \mid W_n$ for all $n \geq \rho$.
- Suppose that ρ (> 3) is the rank of appearance of a prime p in the EDS (W_n). If $m = \nu_p(W_\rho)$, the rank of apparition of p^n in (W_n) is ρ or $p^{n-m}\rho$, according as $n \leq m$ or $n > m$.
- If (W_n) is an EDS in which W_3 and W_4 are coprime, then $\gcd(W_n, W_m) = |W_{\gcd(m,n)}|$.

Ward defined the discriminant Δ of (W_n) to be the quantity given by the somewhat peculiar-looking expression:

$$\begin{aligned}\Delta =& W_4W_2^{15} - W_3^3W_2^{12} + 3W_4^2W_2^{10} - 20W_4W_3^3W_2^7 \\ &+ 3W_4^3W_2^5 + 16W_3^6W_2^4 + 8W_4^2W_3^3W_2^2 + W_4^4.\end{aligned}$$

He called (W_n) *singular* if its corresponding discriminant is zero, and showed in Theorems 19.1 and 22.1 of [34] that any singular (W_n) must be equivalent to the Lucas sequences $(U_n(P,1))$ and that this will not be the case when $\Delta \neq 0$. An example of a nonsingular (W_n) is

$$\begin{aligned} &0,1,1,-1,1,2,-1,-3,-5,7,-4,-23,29,59,129,-314,-65,1529,\\ &-3689,-8209,-16264,83313,113689,-620297,2382785,7869898,\\ &7001471,-126742987,-398035821,1687054711,\cdots \end{aligned} \tag{8.6}$$

This sequence occurs as A006769 in the *Online Encyclopedia of Integer Sequences* (OEIS) [28].

All of this suggests that the EDSs possess properties that Lucas would have found very desirable, except for one important difficulty: in Sect. IX of [34], Ward provides several arguments which suggest that it would be most unlikely for (W_n) to be a linear recurrence sequence (X_n), of order $k = 3$ or 4. This is mainly because the arithmetic behavior of (X_n) is rather different from that of (W_n); in particular, their possible ranks of appearance seemed to be different. He also mentioned that two consecutive terms of a linear recurrence sequence with $k > 2$ can be divisible by a prime p without having almost all terms of the sequence being divisible by p, but that could not be so for (W_n). Thus, although Lucas was looking in what would subsequently turn out to be a very productive direction, his apparent belief that solutions of (8.5) should be linear recurring sequences of order *three* or *four* seemed to ensure his lack of further progress.

To continue with our discussion of elliptic divisibility sequences, we point out that Ward showed, using different language, that any nondegenerate EDS is associated in a specific way with a pair (E,P) made up of an elliptic curve $E/\mathbb{Q}$ and a point $P \in E(\mathbb{Q})$. This correspondence can be given as $W_n = \psi_n(P)$, where $\psi_n(x,y)$ is the n-division polynomial of E. For a given W_2, W_3, W_4, the associated elliptic curve is given explicitly in [34] and, by using more modern notation, in Sect. 10.3 of [8] or the appendix of Silverman and Stephens [26]. For (8.6), the associated elliptic curve $E/\mathbb{Q}$ is modeled by $y^2 + y = x^3 - x$ and P is $(0,0)$. It may appear on a cursory glance that the terms in (8.6) are not growing very quickly, but when P is non-torsion, which is usually the case, it can be shown that the growth rate of the corresponding (non-singular) (W_n) is given by

$$\lim_{n\to\infty} \log |W_n|/n^2 = h > 0,$$

where h is a constant, called the canonical height of P. Since this growth rate is much faster than that of any linear recurrence sequence (X_n), we see another reason why such a (W_n) cannot be a linear recurrence.

Only occasional attention was paid to elliptic divisibility sequences until about 2000, when they were recognized as being members of a class of nonlinear recurrences that are more easily subject to analysis than most such sequences. This manageability comes about from the aforementioned close connection between EDSs and elliptic curves. As a more detailed study of these objects would take us well beyond the scope of this book, the interested reader is referred to Chap. 10 of [8] for a good synopsis of information concerning EDSs and for several references. Further material can be found in the theses of Shipsey [25], Swart [30], and de Looij [15] and the paper of Silverman and Stange [27]. It should be mentioned here that (W_n) is a particular Somos-4 sequence. For $k \geq 4$, a Somos-k sequence (S_n) is generated by the quadratic recurrence relation:

$$S_{n+k}S_n = \sum_{j=1}^{\lfloor k/2 \rfloor} \alpha_j S_{n+k-j}S_{n+j},$$

where α_j, $j = 1, 2, \ldots, \lfloor k/2 \rfloor$, are constants and the initial values $S_0, S_1, \ldots, S_{k-1}$ are given. We can easily deduce from (8.5) that

$$W_{n+4}W_n = W_2^2 W_{n+3}W_{n+1} - W_1 W_3 W_{n+2}^2;$$

thus (W_n) is a Somos-4 sequence for $\alpha_1 = W_2^2$, $\alpha_2 = W_1 W_3$. For more information and references concerning Somos-4 sequences, see the paper of Hone and Swart [10].

We conclude this section by mentioning that Stange [29] has applied EDSs and their higher rank generalizations, called elliptic nets, to cryptography.

8.3 Linear Divisibility Sequences

We have seen in the previous section that Lucas' idea of moving in the direction of elliptic divisibility sequences could have been very productive for him, but, unfortunately, he was laboring under a misconception which prevented further advancement. Also, the state of development of mathematics at the time would likely have precluded his making any significant discoveries, even if he were not burdened by his fixation on linear recurrences. It seems, on perusing what little he did say concerning the problem of generalization, that divisibility sequences would play a prominent role. Certainly, the sequence given by (6.1) and the elliptic sequences both possess this property. In view of the importance of this feature in his development of the arithmetic properties of the Lucas sequence (U_n), this is not surprising. It seems that he might have been searching for linear recurrence sequences which were also divisibility sequences. Indeed, Ward [32], [33] coined the term "Lucasian" for such sequences. In this section we will briefly investigate them.

Let k be a positive integer. As in Sect. 7.1, we let the sequence (X_n) be determined by an initial set of integer values $X_0, X_1, X_2, \ldots, X_{k-1}$ and the linear recurrence:

$$X_{n+k} = P_1 X_{n+k-1} - P_2 X_{n+k-2} + \ldots + (-1)^{k-1} P_k X_n, \tag{8.7}$$

where $P_1, P_2, \ldots, P_k$ are given fixed integers. The sequence (X_n) is said to be a *linear divisibility sequence* (LDS) or a *Lucasian sequence* of order k if $X_n \mid X_{mn}$ whenever $m, n \geq 0$. In what follows we will always use (X_n) to denote a linear divisibility sequence of order k.

In connection with this study, it will be useful to discuss what Koshkin [11] has called a *divisibility polynomial*. We say that a polynomial $f(x)$ with integer coefficients is a divisibility polynomial if $f(x^m)$ divides $f(x^n)$ whenever $m \mid n$. Here m and n denote positive integers. It is easy to see that for $f(x)$ to be a divisibility polynomial, it is necessary and sufficient that $f(x)$ divide $f(x^n)$ for all positive integers n. As examples of divisibility polynomials, we mention $f(x) = x - 1$ or $f(x) = (x+1)(x^m - 1)$ with positive odd m. In [11] the author completely characterizes the divisibility polynomials and uses his results to construct some interesting LDSs. For example, he points out that if we select $f(x) = (x+1)(x^3 - 1)$ and put $x = \alpha/\beta$, where $\alpha + \beta = 1$ and $\alpha\beta = -1$, we find that (X_n) with $X_n = L_n F_{sn}/F_s$, for any fixed odd positive integer s, is a LDS of order four. Similarly, for $f(x) = (x+1)(x^2+1)(x^3-1)$ and $x = \alpha/\beta$, we can see that if $X_n = \frac{1}{6} L_n L_{2n} F_{3n}$, then (X_n) is a LDS of order six.

We next present some simple results, given in Hall[9], concerning any LDS (X_n).

Theorem 120 *If (X_n) is a linear divisibility sequence of order k and some nonzero X_r $(r \geq 0)$ has a factor m relatively prime to P_k, then $m \mid X_0$.*

Proof By results in Sect. 7.1, we know that since $\gcd(m, P_k) = 1$, we have $X_{n+\tau} \equiv X_n \pmod{m}$ for all $n \geq 0$, where τ is the minimal period length of (X_n) modulo m. Hence, $X_\tau \equiv X_0 \pmod{m}$. It also follows by induction on h that $X_{h\tau} \equiv X_\tau \pmod{m}$ for all $h \geq 0$. Thus, $X_{r\tau} \equiv X_0 \pmod{m}$, but since (X_n) is a divisibility sequence, we must have $X_r \mid X_{r\tau}$, which means that we must have $m \mid X_0$. □

Corollary 121 If $X_0 \neq 0$, then any prime which divides some nonzero term of (X_n) must be a divisor of $\gcd(X_0, P_k)$. □

Thus, when $X_0 \neq 0$, there can only be a finite number of primes which can divide all of the terms of (X_n). However, when $X_0 = 0$, then any prime which does not divide P_k will occur as a divisor of infinitely many terms of (X_n). It is for this reason that we will assume that $X_0 = 0$ in (X_n); also, since (X_n) is a divisibility sequence, we must have $X_1 \mid X_n$ for all $n > 0$. Thus, if $X_1 = 0$, then $X_n = 0$ for all $n > 0$, and the resulting sequence is not very

interesting. We exclude such sequences from consideration. When $X_1 \neq 0$, then (X_n/X_1) is a linear divisibility sequence of order k; hence, there is no loss of generality in assuming that $X_1 = 1$. Such a divisibility sequence is said to be *normalized*.

We can now generalize the idea of a primitive divisor introduced in Sect. 4.4. We will say that a prime p, which does not divide P_k, is a *primitive divisor* of X_h, a term of (X_n), if p divides X_h, but $p \nmid X_r$ for $0 < r < h$. We have the following theorem.

Theorem 122 *If p is a primitive divisor of X_h, then $h \mid \tau(p)$.*

Proof We let $d = \gcd(h, \tau)$, where we will denote $\tau(p)$ by τ here. There must exist positive integers x, y such that $hx - \tau y = d$. Since (X_n) is a divisibility sequence, we must have $p \mid X_{xh}$. Also, by the definition of τ, we must have $0 \equiv X_{xh} \equiv X_{xh-\tau y} = X_d \pmod{p}$. As p is a primitive divisor of X_h, we see that we can only have $d \geq h$; hence, $d = h$ and $d \mid \tau$. □

Further properties of LDSs where the discriminant of the characteristic polynomial is not zero were proved in Ward [31], but little progress was made on the problem of determining the LDSs (if any exist) for a given characteristic polynomial. In what follows we will assume that the LDS (X_n) is nondegenerate; that is, no quotient of any two of the roots of its characteristic polynomial is a root of unity. This means that the polynomial cannot have two roots to a common power that are equal.

Now suppose $f(x)$ and $g(x)$ are given by

$$f(x) = x^k - P_1 x^{k-1} + P_2 x^{k-2} - \ldots + (-1)^k P_k,$$
$$g(x) = x^h - Q_1 x^{h-1} + Q_2 x^{h-2} - \ldots + (-1)^h Q_h,$$

where P_i $(i = 1, 2, \ldots, k)$ and Q_i $(i = 1, 2, \ldots, h)$ are integers and the discriminants of $f(x)$ and $g(x)$ are both nonzero. Let $\rho_1, \rho_2, \ldots, \rho_k$ be the roots of $f(x)$ and $\sigma_1, \sigma_2, \ldots, \sigma_h$ the roots of $g(x)$. Recall that the *resultant of f and g*, written $R(f, g)$, satisfies

$$R(f, g) = \prod_{i=1}^{k} g(\rho_i).$$

If we let $f_n(x)$ be the polynomial with roots $\rho_1^n, \rho_2^n, \ldots, \rho_k^n$ and $g_n(x)$ the polynomial with roots $\sigma_1^n, \sigma_2^n, \ldots, \sigma_h^n$. We can put $R_n = R(f_n, g_n)$. If all the roots $\rho_1, \rho_2, \ldots, \rho_k$, $\sigma_1, \sigma_2, \ldots, \sigma_h$ are distinct, we can define r_n by $r_n = R_n/R_1$. Ward [32] remarked that when $n \geq 1$, r_n is an integer. Also (r_n) is a linear recurrence sequence which is also a divisibility sequence and is therefore a Lucasian sequence; Ward called (r_n) an R-sequence. He was unable to find any Lucasian sequence which was not an R-sequence; indeed, he stated that "it appears probable that all Lucasian sequences may be exhibited as R-sequences or divisors of R-sequences." This was pretty much the way matters

stood until 1990 when Bézivin, Pethö, and van der Poorten [6] were able to prove Ward's statement.

We can write r_n above as

$$r_n = \prod_{i=1}^{k} \prod_{j=1}^{h} \frac{\rho_i^n - \sigma_j^n}{\rho_i - \sigma_j}. \tag{8.8}$$

In [6], the authors observe that even if all the roots $\rho_1, \rho_2, \ldots, \rho_k, \sigma_1, \sigma_2, \ldots, \sigma_h$ are not distinct, by using reasoning similar to that in Sect. 2.1, on each term of the above product (8.8), the generalized R-sequence r_n can be put in the form:

$$r_n = n^m \gamma^{n-1} \prod_i (\alpha_i^n - \beta_i^n)/(\alpha_i - \beta_i). \tag{8.9}$$

Here γ, α_i, β_i represent fixed nonzero algebraic numbers and m is some nonnegative integer. By making use of deep results in the theory of exponential polynomials and the Hadamard quotient theorem, they were able to prove the following result.

Theorem 123 *If (X_n) is a nondegenerate LDS, then there exists a resultant sequence (r_n) of the form:*

$$r_n = n^m \prod_i (\alpha_i^n - \beta_i^n)/(\alpha_i - \beta_i), \tag{8.10}$$

such that for all $n > 0$, we must have $X_n \mid r_n$.

Recently, by making use of the theory of generalized Vandermonde determinants, Barbero [3] was able to give an elementary proof of a more precise version of Theorem 123. We give below his result in the specific case where the characteristic polynomial of (X_n) has a nonzero discriminant, but his overall result is much more general than this.

Theorem 124 *If (X_n) is a nondegenerate LDS of degree k whose characteristic polynomial has roots $\rho_1, \rho_2, \ldots, \rho_k$, then for all $n \geq 0$, we must have $X_n \mid r_n$, where*

$$r_n = \prod_{1 \leq i < j \leq k} \frac{\rho_i^n - \rho_j^n}{\rho_i - \rho_j}.$$

Notice that r_n here is the same as Lucas' $\Delta(\rho_1^n, \rho_2^n, \ldots, \rho_k^n)/\Delta(\rho_1, \rho_2, \ldots, \rho_k)$ in (6.1).

Theorem 124 was used by Abrate et al. [1] to prove the following pretty result.

Theorem 125 *If (X_n) is a nondegenerate LDS of degree 4, then its characteristic polynomial must be of the form:*

$$x^4 - Px^3 + (R + 2Q)x^2 - PQx + Q^2,$$

for some integers P, Q, R.

The above polynomial is the characteristic polynomial $F(x)$ for the extended Lehmer functions in Sect. 7.3 when $k = 2$ and $R = P_2$. This is not a coincidence because in this case, $x_n = V_{1,n}$ and (x_n) is a divisibility sequence. We will discuss this further in the next section.

Unfortunately, Theorem 124 only provides us with a sequence whose terms must be divisible by those of (X_n), but does not give us a formulation for X_n. In [18] Oosterhout made the following interesting conjecture (Conjecture 3.5.6).

Conjecture 126 Let (X_n) be any nondegenerate LDS and let $\rho_1, \rho_2, \ldots, \rho_k$ be the roots of its characteristic polynomial. Let Γ be the subgroup of the group of all nonzero algebraic numbers generated by the ρ_i. Then, there exists some $c \in \overline{\mathbb{Q}}$, elements $\lambda, \gamma_1, \gamma_2, \ldots, \gamma_m$ in Γ and divisibility polynomials $p_1, p_2, \ldots, p_m$ such that

$$X_n = c\lambda^n p_1(\gamma_1^n) p_2(\gamma_2^n) \ldots p_m(\gamma_m^n),$$

for all $n \geq 0$. □

In the case that Γ is non-torsion, a sketch of the statement and a rather rough proof of this conjecture can be found in Sect. 5 of Everest and van der Poorten [7].

The difficulty with using this conjecture is that it is only a necessary condition on X_n. For any given value of k, it provides little information about what the values of λ, $\gamma_1, \gamma_2, \ldots, \gamma_m$ should be; nevertheless, Oosterhout was able to make use of it to characterize conditionally all the LDSs of order 2, 3, and some of order 4. Recall, however, that we saw in Sect. 6.2 that we still have no proof concerning the identity of the LDSs of order three; thus, this conjecture, if true, is likely very difficult to prove. If we put $m = k$, $p_i(x) = x - 1$ $(i = 1, 2, \ldots, k)$ and insist that $X_1 = 1$, we get:

$$X_n = \lambda^{n-1} \prod_{i=1}^{k} (1 - \gamma_i^n)/(1 - \gamma_i),$$

a sequence we will consider in the next section.

8.4 Extended Lucas Sequences

In Roettger et al. [23], it is argued that the Lucas sequences can be characterized by four basic properties:

(1) There are two sequences of integers (when $n \geq 0$).
(2) Both sequences satisfy the same linear recurrence relation.

(3) One of the two sequences is a divisibility sequence.

(4) There are both addition and multiplication formulas for the terms of the sequences. These are identities respectively of the type $X_{m+n} = \cdots$, $X_{mn} = \cdots$, where the right-hand sides are polynomial expressions involving the mth and nth terms of the sequences in (1).

Given what we do know about Lucas' attempt to generalize his sequences, it seems that any sequences which he might have found acceptable as a proper generalization of U and V should possess these four properties. We remark that Roettger's sequences in Sect. 6.6 do satisfy these four properties, but are there any others?

One candidate is the Pierce sequences. In 1916 Pierce [19] produced two sequences with properties very similar to Lucas' U and V. He denoted these by (Δ_n) and (S_n), where

$$\Delta_n = \prod_{i=1}^{k}(1-\rho_i^n) \text{ and } S_n = \prod_{i=1}^{k}(1+\rho_i^n).$$

Here $\rho_1, \rho_2, \ldots, \rho_k$ are the roots of a monic polynomial $f(x)$ of degree k with integral coefficients. He was able to derive a number of features of these sequences which are very similar to those of Lucas' (U_n) and (V_n). For example, he showed that (Δ_n) is a divisibility sequence. He also obtained several number theoretic results concerning these sequences, particularly when the degree of $f(x)$ is three. Later, Lehmer [12] extended some of Pierce's results, showing, among other things, that each satisfies a linear recurrence relation. Indeed, Lehmer [13] employed these functions in a test, which makes use of the factors of $N^2 + N + 1$ to demonstrate the primality of N. Unfortunately, Pierce's functions are difficult to compute, which means that using them is not very practical. (Lehmer explains this in detail on pages 50–60 in his unpublished 1968 notebook #11, which, together with all the rest of his notebooks, is now in the Bancroft Library at U.C. Berkeley.) While Pierce's work certainly produced a kind of extension of the Lucas functions, it is very unlikely that Lucas was thinking along these lines, because nowhere in his work does he allude to anything like these sequences. Also, Pierce's sequences do not become (U_n) and (V_n) when $f(x)$ is of degree two.

In [23] the authors, on considering Conjecture 126 and (8.9), generalized Pierce's S_n and a normalized version of his Δ_n by putting

$$U_n = \lambda^{n-1}\prod_{i=1}^{k}\frac{1-\gamma_i^n}{1-\gamma_i} \text{ and } V_n = \lambda^n\prod_{i=1}^{k}(1+\gamma_i^n), \tag{8.11}$$

where λ and $\gamma_1, \gamma_2, \ldots, \gamma_k$ are simply constrained to be nonzero algebraic numbers such that $V_1 \neq 0$ and both (U_n), (V_n) are sequences of integers

for $n \geq 0$. Notice that, just as in the case of the Lucas sequences, we have $V_n = U_{2n}/U_n$.

Under the above constraints, it is easy to prove that if $k = 1$, $P = \lambda(\gamma_1+1)$, $Q = \lambda^2\gamma_1$, then both P and Q must be integers because $V_1 = \lambda(\gamma_1 + 1)$, $V_2 = \lambda^2(1 + \gamma_1^2)$, $U_3 = \lambda^2(1 + \gamma_1 + \gamma_1^2)$ are all integers. In this case, we see that in (8.11) $U_n = U_n(P, Q)$, $V_n = V_n(P, Q)$, where $\alpha = \lambda$ and $\beta = \lambda\gamma_1$. Thus, (8.11) represents a generalization of the Lucas functions.

For any fixed value of k, conditions on λ and $\gamma_1, \gamma_2, \ldots, \gamma_k$ are derived in [23] to ensure that both (U_n) and (V_n) are sequences of integers which satisfy the same linear recurrence. For example, one of these conditions is that Q $(= \lambda^2\gamma_1\gamma_2 \ldots \gamma_k)$ be an integer. It is also shown that under these same conditions, (U_n) is a divisibility sequence. In the case that $k = 2$, we must have T_1, T_2, and Q integers, where

$$T_1 = \lambda(1+\gamma_1)(1+\gamma_2),\ T_2 = \lambda^2(\gamma_1+\gamma_2)(1+\gamma_1\gamma_2)+2\lambda^2\gamma_1\gamma_2 \text{ and } Q = \lambda^2\gamma_1\gamma_2.$$

Thus, if we put $P_1 = T_1$ and $P_2 + 2Q = T_2$, we must have P_1, P_2 and Q integers. In this case we find that both (U_n) and (V_n) satisfy the fourth-order linear recurrence:

$$X_{n+4} = P_1X_{n+3} - (P_2 + 2Q)X_{n+2} + P_1QX_{n+1} - Q^2X_n,$$

with initial conditions $U_0 = 0$, $U_1 = 1$, $U_2 = P_1$, $U_3 = P_1^2 - P_2 - 3Q$, $V_0 = 4$, $V_1 = P_1$, $V_2 = P_1^2 - 2P_2 - 4Q$, $V_3 = P_1(P_1^2 - 3P_2 - 3Q)$. Notice that the characteristic polynomial for (X_n) is the polynomial in Theorem 125. We have:

$$U_n = V_{1,n} \text{ and } V_n = 2V_{0,n} + P_1V_{1,n}, \tag{8.12}$$

where $(V_{0,n})$ and $(V_{1,n})$ are the generalized Lehmer sequences for $k = 2$ in Sect. 7.3. The sequences (U_n) and (V_n) were discussed in some detail by Williams and Guy in [37], [38], and further properties of them were developed in Roettger et al. [24]. Suffice it to say here that they possess the four properties of the Lucas sequences mentioned at the beginning of this section. There is also a law of repetition, a law of appearance, and a Fundamental theorem analogous to those for the Lucas sequences. Thus, these are evidently the fourth-order analogues of the Lucas sequences.

When $k = 3$, the situation is somewhat more complicated because the sequences satisfy a linear recurrence of order 8; this is given in Theorem 5.3 of [23]. A difficulty, however, arises when we try to develop the addition and multiplication formulas because it becomes necessary to introduce a third sequence in order to do this; thus, the sequences when $k = 3$ cannot in general satisfy the four conditions given earlier. This, of course, is also likely the case for $k > 3$. Nevertheless, there is a special case when $k = 3$ which does allow us to require only two sequences; this is the case when $\gamma_1\gamma_2\gamma_3 = 1$. Here we must have λ an integer, denoted by R, and the resulting sequences (U_n) and $(V_n - 2R^n)$ satisfy the same linear recurrence of order six:

$$\begin{aligned} X_{n+6} =& S_1 X_{n+5} - (S_2 + 3R^2) X_{n+4} + (S_3 + 2R^2 S_1) X_{n+3} \\ & - R^2 (S_2 + 3R^2) X_{n+2} + R^4 S_1 X_{n+1} - R^6 X_n, \end{aligned} \tag{8.13}$$

where S_1, S_2, and S_3 are integers such that

$$S_3 = RS_1^2 - 2RS_2 - 4R^3. \tag{8.14}$$

In this case it turns out that ρ_1, ρ_2, ρ_3, where $\rho_i = R(\gamma_i + \gamma_i^{-1})$ $(i = 1, 2, 3)$, are the roots of the cubic polynomial:

$$x^3 - S_1 x^2 + S_2 x - S_3.$$

If we put $W_n = V_n - 2R^n$, it is shown in [23] that (U_n) and (W_n) also possess the four properties mentioned at the beginning of this section. Also, if we put $Q = R^2$, $P_1 = S_1$, $P_2 = S_2$, $P_3 = S_3$, we see that (8.13) is the recurrence for the generalized Lehmer functions when $k = 3$. By using formulas in Sect. 7 of [23], it can be shown that

$$U_n = U_2 U_{1,n} + U_3 U_{2,n} \text{ and } W_n = 3V_{0,n} + P_1 V_{1,n} + (P_1^2 - 2P_2) V_{2,n}, \tag{8.15}$$

where $U_2 = P_1 + 2R$, $U_3 = P_1^2 + RP_1 - P_2 - 3R^2$. When $k = 3$ and $P_3 = RP_1^2 - 2RP_2 - 4R^3$, this provides the connection similar to (8.12) (in the $k = 2$ case) between the (U_n) and (W_n) sequences, and the corresponding generalized Lehmer sequences.

The arithmetic theory of the (U_n) and (W_n) sequences defined here is very rich and would certainly have appealed to Lucas. Several arithmetic results concerning them can be found in [23] and in Roettger and Williams [20]. Indeed, it has been shown by Roettger and Williams [21] that special instances of these sequences can be used to produce a necessary and sufficient primality test for integers N such that $N^6 - 1$ is divisible by a large power of 7. Given some prime q $(\equiv 1 \pmod 7)$ such that $N^{(q-1)/7} \not\equiv 1 \pmod N$, this test executes in $O(\log N)$ modular multiplications modulo N and is very similar to a $p = 7$ version of the general test of Theorem 118, but is more strictly analogous to the $p = 5$ test of Theorem 119.

We also point out that if P, Q, R are arbitrary integers and we put $S_1 = PQ - 3R$, $S_2 = P^3R + Q^3 - 5PQR + 3R^2$, $S_3 = R(P^2Q^2 - 2Q^3 - 2P^3R + 4PQR - R^2)$, then S_1, S_2, S_3 satisfy (8.14) and the corresponding (U_n) and (W_n) are the Roettger sequences discussed in Sect. 6.6.

We have seen in this section that Lucas' intuition was correct about the existence of fourth-order extensions of his sequences. It seems that he was wrong about the existence of third-order analogues which satisfy a cubic recurrence, but there are sixth-order analogues, and the roots of cubic polynomials play a role in this theory, particularly for Roettger's sequences. Of course, there exist further sequences for $k > 3$, but it seems very likely that Condition (1) will be violated. This, however, should not be regarded as a significant

obstacle to further advancement of the theory. Indeed, in the general case of $k = 3$, only a third function is required in dealing with linear recurrences of order eight. It would be of some interest to discover what further results might be derived for the sequences given by (8.11) when $k \geq 3$.

8.5 Odd and Even Extensions of the Lucas Sequences

Consider a linear recurring sequence (X_n) with characteristic polynomial $F(x)$ of even degree $2k$ having zeros α_i, β_i such that $\alpha_i\beta_i = Q$ $(i = 1, \ldots, k)$. By analogy to similar definitions in the theory of functions, we say that (X_n) *is even* if $X_{-n} = X_n/Q^n$ and (X_n) *is odd* if $X_{-n} = -X_n/Q^n$ for all integral values of n. For example, $(U_n(P, Q))$ is odd and $(V_n(P, Q))$ is even by (2.7); also, by (10.2.3) of [36], the generalized Lehmer sequences $(U_{i,n})$ $(i = 1, 2, \ldots, k)$ are all odd and $(V_{i,n})$ $(i = 1, 2, \ldots, k)$ are all even. Hence, the fourth- order LDS (U_n) mentioned in the last section is even. Let D be the discriminant of $F(x)$ and suppose that $D \neq 0$. It not very difficult to see that (X_n) is even if and only if

$$X_n = c_1(\alpha_1^n + \beta_1^n) + c_2(\alpha_2^n + \beta_2^n) + \ldots + c_k(\alpha_k^n + \beta_k^n);$$

and (X_n) is odd if and only if

$$X_n = c_1(\alpha_1^n - \beta_1^n) + c_2(\alpha_2^n - \beta_2^n) + \ldots + c_k(\alpha_k^n - \beta_k^n).$$

Here the c_i $(i = 1, 2, \ldots, k)$ are constants determined by the initial conditions on (X_n). These results are proved in Sect. 2 of Williams and Guy [39].

The object of [39] was to find which of the linear divisibility sequences of order four are either even or odd. The discussion there was confined to LDSs with characteristic polynomial of the form

$$F(x) = x^4 - Px^3 + (R + 2Q)x^2 - PQx + Q^2, \tag{8.16}$$

but as we have seen in Theorem 125, these are the only nondegenerate LDSs of order four. By (7.21), the discriminant of (8.16) is $D = E\Delta^2Q^2$, where $\Delta = P^2 - 4R$ and $E = (R + 4Q)^2 - 4QP^2$.

It is by no means clear that any nondegenerate LDS of order four must be either even or odd; in fact, when $P = 0$, there exist fourth-order LDSs which are neither even nor odd. For example, consider $P = 0$, $R = Q = -1$; we get $X_n = F_n$ when n is even and $X_n = L_n$ when n is odd. It follows since $X_{-m} = X_m/Q^m$ when m is odd and $X_{-m} = -X_m/Q^m$ when m is even, that (X_n) can be neither even nor odd; nevertheless, (X_n) is a nondegenerate fourth order divisibility sequence. However, it is also true in this case that we can represent X_n as $\bar{U}_n(5, 1)$, which is an odd fourth-order divisibility

sequence for $Q = 1$. In general, when $P = 0$, then either (X_n) is odd for a given Q or, if not, it is when we replace Q by $-Q$.

Note that if (X_n) is any odd fourth-order LDS, then it is completely determined once we know X_2, because we must have $X_{-1} = -1/Q$, $X_0 = 0$ and $X_1 = 1$; in fact, it is easy to show that the terms in such a sequence will always be of the form $X_n = U_{0,n} + X_2 U_{1,n}$ for the $(k = 2)$ generalized Lehmer functions with characteristic polynomial (8.16). However, this is only a necessary condition and is not sufficient.

Let $\Delta = Su^2$ and $E = Gv^2$, where S, G, u, v are integers and S and G are both square-free. Let (X_n) be any non-null linear divisibility sequence with characteristic polynomial $F(x)$ given by (8.16) with $D \neq 0$ and $P \neq 0$. In [39] the following results are proved:

- There is one and only one even (X_n) for any given $F(x)$;
- If $S \neq 1$ and $G \neq 1$, (X_n) is either even or odd;
- If $S \neq 1$ and $G \neq 1$ and $G \neq S$, there can be no odd (X_n);
- If $S = 1$ and $G \neq 1$, then the only possible odd (X_n) is a fundamental Lucas sequence.

We have already seen that the sequence in the first bullet is the sequence (U_n), mentioned in the previous section $(k = 2)$, whose first four terms are 0, 1, P, $P^2 - R - 3Q$. Such a sequence is called *standard* in [1]; it is shown there that it can always be written as the product of two Lucas-like functions. These two functions can be expressed as $(\alpha_1^n - \beta_1^n)/(\alpha_1 - \beta_1)$ and $(\alpha_2^n - \beta_2^n)/(\alpha_2 - \beta_2)$, where

$$\alpha_1 + \beta_1 = (A \pm B)/(2\sqrt{Q}),\ \alpha_1\beta_1 = Q,\ \alpha_2 + \beta_2 = (A \mp B)/(2\sqrt{Q}),\ \alpha_2\beta_2 = Q,$$

and $A = \sqrt{R + 4Q + 2P\sqrt{Q}}$, $B = \sqrt{R + 4Q - 2P\sqrt{Q}}$.

While we emphasize that this has not yet been proved, it appears that there are no nondegenerate odd fourth-order LDSs when $G = S \neq 1$ or when $S \neq 1$ and $G = 1$. Thus, considering the above results, we could only expect to find an odd fourth-order LDS (X_n) when $G = S = 1$.

If $G = 1$, it is shown in [38] that $P^2 = r_1 r_2$, $R = q_1 r_2 + q_2 r_1 - 4q_1 q_2$, $Q = q_1 q_2$ and $E = (q_1 r_2 - q_2 r_1)^2$, where r_1, q_1, r_2, q_2 are integers such that $r_1 > 0$, $r_2 > 0$, $\gcd(r_1, q_1) = 1$, $\gcd(r_2, q_2) = 1$ and $r_1 r_2$ is a perfect square. If $G = 1$ and (X_n) is even, then it is also shown in [38] that

$$|X_n| = |U_n(\sqrt{r_1}, q_1)\, U_n(\sqrt{r_2}, q_2)|.$$

From results in Sect. 4.4, it follows that the sequence (X_n) is clearly a divisibility sequence. Thus, if $G = 1$ (E is a perfect integral square) and (X_n) is even, then (X_n) must be a LDS of order four.

If $G = 1$ and $S \neq 1$, it is shown in [39] that any odd fourth-order LDS (X_n) must have the form:

$$X_n = V_n(\sqrt{r_1}, q_1)U_n(\sqrt{r_2}, q_2)/\sqrt{r_1},$$

where (X_n) satisfies the fourth-order linear recurrence

$$X_{n+4} = PX_{n+3} - (R + 2Q)X_{n+2} + QPX_{n+1} - Q^2X_n,$$

but it is not always the case that this (X_n) will be a divisibility sequence. For example, if $r_1 = r_2 = 7$, $q_1 = 2$ and $q_2 = 141002$, we see that (X_n) behaves like a divisibility sequence until we arrive at the 28th term, where we discover that X_{14} is not a divisor of X_{28}. However, if we put $r = r_1$, $q = q_1$, $r_2 = V_s(\sqrt{r}, q)^2 = r\bar{V}_s(r, q)^2$ and $q_2 = q_s$, where s is any fixed odd positive integer, we get:

$$X_n = \bar{V}_n(r, q)\bar{U}_{ns}(r, q)/\bar{U}_s(r, q).$$

Here $\bar{U}$ and $\bar{V}$ denote the Lehmer sequences. (This X_n is essentially the same function as that discovered by Koshkin when $f(x) = (x + 1)(x^3 - 1)$ and $x = \alpha/\beta$, where $\alpha + \beta = \sqrt{r}$ and $\alpha\beta = q$.) It can be shown that this (X_n) is a fourth-order odd LDS with characteristic polynomial (8.16); also, by using some identities which are satisfied by the Lehmer functions (Sect. 4.4), we have $P = r\bar{V}_s(r, q)$, $R = q\bar{V}_{s-1}(r, q)\bar{V}_{s+1}(r, q)$, $Q = q^{s+1}$, $\Delta = (r - 4q)^2\bar{U}_s(r, q)^2$, $E = \big(qr(r - 4q)\bar{U}_{s-1}(r, q)\bar{U}_{s+1}(r, q)\big)^2$, and $X_2 = (r - 2q)\bar{V}_s(r, q)$. Notice that in this case, we have $S = 1$.

In the particular case of $s = 3$, we have $P = r(r - 3q)$, $R = q(r - 2q)(r^2 - 4rq + 2q^2)$, $Q = q^4$ and $X_2 = (r - 2q)(r - 3q)$, whereas for the standard sequence, we would have $X_2 = P = r(r - 3q)$. If we put $r = 5$ and $q = 1$, we get $P = 10$, $R = 21$, $Q = 1$, the standard sequence $(L_{4n} - L_{2n})/4$ with terms

$$0,1,10,76,540,3751,25840,177451,1217160,8344876,$$
$$57202750,392089501,\cdots,$$

and the odd sequence $(F_{4n} + F_{2n})/4$ with terms

$$0,1,6,38,252,1705,11628,79547,544824,3733234,25585230,175356611,\cdots$$

These are listed as A215465 and A215466, respectively, in the OEIS. As noted in [37], the terms of the sequence A215465 can be written as $L_nF_{3n}/4$ when n is even and $F_nL_{3n}/4$ when n is odd. This same sequence was also produced by Bala [2], using a different procedure.

The above sequence with different values for r and q will also yield the odd LDSs: A238536 ($r = 1$, $q = -1$), A238537 ($r = 4$, $q = -1$), and A238538 ($r = 9$, $q = 2$).

If we next select (X_n) here by setting $X_2 = r(r - 2q)$, then it turns out that this (X_n) is also an odd fourth- order LDS with characteristic polynomial (8.16) and, as before, $P = r(r - 3q)$, $R = q(r - 2q)(r^2 - 4rq + 2q^2)$, $Q = q^4$. Here, it can be shown that

$$X_n = \bar{U}_{2n}(r,q)U_n(\sqrt{r},q)^2.$$

If we put $r = 5$, $q = 1$, we get the sequence:

$$0, 1, 15, 128, 945, 6655, 46080, 317057, 2176335, 14925184, 102320625, \cdots,$$

of general term $F_{4n} - 2F_{2n}$, which appears as A127595 in the OEIS.

If we put $r_1 = t^2$, $q_1 = q$, $r_2 = (t^2 - 2q)^2$, $q_2 = q^2$ and $X_2 = t^3$, we find that $\Delta = t^2(t^2 - 4q)^2$ and $X_n = U_n(t,q)^3$. The corresponding sequence (X_n) is clearly odd and a fourth-order LDS. For $t = 1$, $q = -1$, we get A056570 in the OEIS.

Most of the above sequences were found, using a different approach, by Oosterhout [18]. Also, the Lehmer sequence $\bar{U}$ is a fourth-order linear divisibility sequence as is $(a_n\bar{U}_n(R,Q))$, where (a_n) is a special periodic sequence of integers such that $a_1 = 1$ and $a_n \mid a_{2n}$. Indeed, the a sequence must be some $\bar{V}$ sequence, where $Q = \pm 1$ and $R = Q$, $2Q$ or $3Q$.

We have seen, then, that there are infinitely many odd fourth-order LDSs; are there any others apart from those mentioned here? Possibly, the answer to this question is yes, but no nontrivial examples are known to the authors, none were found during an extensive computer search and none appear in the OEIS. For more information concerning fourth-order odd divisibility sequences, see Roettger and Williams [22].

When $k = 3$, we have seen that if $Q = R^2$ and $P_3 = RP_1^2 - 2RP_2 - 4R^3$, the sixth-order linear recurrence

$$\begin{aligned} X_{n+6} =& P_1X_{n+5} - (P_2 + 3Q)X_{n+4} + (P_3 + 2QP_1)X_{n+3} \\ & - Q(P_2 + 3Q)X_{n+2} + Q^2P_1X_{n+1} - Q^3X_n \end{aligned} \tag{8.17}$$

is satisfied by the divisibility sequence (U_n), where $U_0 = 0$, $U_1 = 1$, $U_2 = P_1 + 2R$, $U_3 = P_1^2 + RP_1 - P_2 - 3R^2$. Since the generalized Lehmer sequences $(U_{i,n})$ $(i = 1, 2, 3)$ are all odd, we see by (8.15) that (U_n) is an odd LDS of order six. Thus, we need only know the values of U_2 and U_3 and (8.17) to completely specify the sequence. Particular instances of this sequence occur in the OEIS as A180510 with $P_1 = -1$, $P_2 = -5$, $R = 1$, $P_3 = 7$ and A005120 with $P_1 = -3$, $P_2 = 2$, $R = 1$, $P_3 = 1$. Others are: A001351, A001945 and A006235.

Apart from the above, very little seems to be known about LDSs of order 6. However, if we have integers Q, L, S such that $L^2 \mid S^2Q$ and put $P_1 = L + S$, $P_2 = LS + T$, $P_3 = LT$, where $T = L^2 + QS^2/L^2 - 4Q$, then it can be shown that the sequence of integers $(X_n)_{n\geq 0}$ with

$$X_n = U_n(L,Q)U_n(\sqrt{(S + 2L)/L}, 1)^2$$

is an odd sixth-order LDS which satisfies (8.17). We remark that this sequence is of the form given in the first formula of (8.11) with $\gamma_1 \neq \gamma_2 = \gamma_3$. There

are several examples of these sequences listed in the OEIS. For example, if we put $L = 6$, $Q = 1$, $S = 42$, we get A003755; others are A003753, A003767, A006235, A006237, and A169630. We also mention Koshkin's sixth-order LDS (X_n) with

$$X_n = \big(V_n(P,Q)V_{2n}(P,Q)U_{3n}(P,Q)\big)/\big(V_1(P,Q)V_2(P,Q)U_3(P,Q)\big).$$

Putting $P = 1$, $Q = -1$, we get $X_n = L_n L_{2n} F_{3n}/6$.

References

1. M. Abrate, S. Barbero, U. Cerutti and N. Murru, *Linear divisibility sequences and Salem numbers*, Pub. Math. Debrecen **91** (2017), 247–259.
2. P. Bala, *A Family of Linear Divisibility Sequences of Order Four*, unpublished MS, Feb. 2014. OEIS A238536.
3. S. Barbero, *Generalized Vandermonde determinants and characterization of divisibility sequences*, J. of Number Theory **173** (2017), 371–377.
4. E. T. Bell, *Analogies between the u_n, v_n of Lucas and elliptic functions*, Bull. Amer. Math. Soc. **29** (1923), 401–406.
5. E. T. Bell, *Letter to professor D. Harkin from E. T. Bell*, Copy in possession of H. C. Williams, 1930.
6. J.-P. Bézivin, A. Pethö and A. J. van der Poorten, *A full characterization of divisibility sequences*, Amer. J. Math. **112** (1990), 985–1001.
7. G. R. Everest and A. J. van der Poorten, *Factorisation in the ring of exponential polynomials*, Proc. AMS **125.5** (1997), 1293–1298.
8. Graham Everest, Alf van der Poorten, Igor Shparlinski, Thomas Ward, *Recurrence Sequences*, Mathematical Surveys and Monographs **104**, AMS, Providence RI, 2003.
9. M. Hall, *Divisibility sequences of the third order*, Amer. J. Math. **58** (1936), 577–584.
10. A. Hone and C. Swart, *Integrality and the Laurent phenomenon for Somos 4 and Somos 5 sequences*, Math. Proc. Cambridge Philos. Soc. **145** (Part I), (2008), no. 1, 65–85.
11. S. Koshkin, *Non-classical linear divisibility sequences and cyclotomic polynomials*, Fibonacci Quart. **57** (2019), 68–80.
12. D. H. Lehmer, *Factorization of certain cyclotomic functions*, Annals of Math. **34** (1933), 461–479.
13. D. H. Lehmer, *The economics of number theoretic computations*, Computers in Number Theory, Academic Press, London, 1971, 1–9.
14. D. H. Lehmer, *The mathematical work of Morgan Ward*, Math. Comp. **61** (1993), 307–311.

15. Rutger de Looij, *Elliptic Divisibility Sequences*, Master's Thesis, University of Utrecht, 2010.
16. É Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. of Math. **1** (1878), 184–240, 289–321.
17. É. Lucas, *Sur la théorie des fonctions numériques simplement périodiques*, Nouvelle Correspondance Mathématique **4** (1878), 1–8.
18. A. D. Oosterhout, *Characterization of divisibility sequences*, Master's Thesis, Utrecht University, June 2011.
19. T. A. Pierce, *The numerical factors of the arithmetic forms* $\prod_{i=1}^{n}(1 \pm \alpha_i^m)$, Annals of Math. **18** (1916), 53–64.
20. E. Roettger and H. C. Williams, *Some arithmetic properties of certain sequences*, J. of Integer Sequences **18** (2015), Article 15.6.2.
21. E. L. Roettger and H. C. Williams, *A sextic extension of the Lucas functions*, J. of Integer Sequences **23** (2020), Article 20.4.8.
22. E. L. Roettger and H. C. Williams, *Appearance of primes in fourth-order odd divisibility sequences*, J. of Integer Sequences **24** (2021), Article 21.7.5.
23. E. Roettger, H. C. Williams and R. K. Guy, *Some extensions of the Lucas functions*, Number Theory and Related Fields: In Memory of Alf van der Poorten, Springer Proceedings in Mathematics and Statistics 43, Springer Science and Business Media, New York, 2013, 271–311.
24. E. Roettger, H. C. Williams and R. K. Guy, *Some primality tests that eluded Lucas*, Designs, Codes and Cryptography **77** (2015), 515–539.
25. R. Shipsey, *Elliptic Divisibility Sequences*, Ph. D. Thesis, Goldsmith's (University of London), 2000.
26. J. H. Silverman and N. Stephens, *The sign of an elliptic divisibility sequence*, J. Ramanujan Math. Soc. **21** (2006), 1–17.
27. J. H. Silverman and K. E. Stange, *Terms in elliptic divisibility sequences divisible by their indices*, Acta Arith. **146** (2011), 355–378.
28. N. J. A. Sloane, editor, *The On-Line Encyclopedia of Integer Sequences*, published electronically at https://oeis.org
29. K. E. Stange, *The Tate pairing via elliptic nets*, Pairing-Based Cryptography (Tokyo, 2007), LNCS 4575, 4575 Springer, Berlin, 2007, 329–348.
30. C. Swart, *Elliptic Curves and Related Sequences*, Ph. D. Thesis, Royal Holloway (University of London), 2003.
31. M. Ward, *Linear divisibility sequences*, Trans. Amer. Math. Soc. **41** (1937), 276–286.
32. M. Ward, *The law of apparition of primes in a Lucasian sequence*, Trans. Amer. Math. Soc. **44** (1938), 68–86.
33. M. Ward, *Arithmetical properties of sequences in rings*, Annals of Math. **39** (1938), 210–219.
34. M. Ward, *Memoir on elliptic divisibility sequences*, Amer. J. of Math. **70** (1948), 31–74.
35. M. Ward, *The law of repetition of primes in an elliptic divisibility sequence*, Duke Math. J. **15** (1948), 941–946.

36. H. C. Williams, *Édouard Lucas and Primality Testing*, Canadian Math. Soc. Series of Monographs and Advanced Texts, John Wiley and Sons, NY, 1998.
37. H. C. Williams and R. K. Guy, *Some fourth order linear divisibility sequences*, Int. J. of Number Theory **7** (2011), 1255–1277.
38. H. C. Williams and R. K. Guy, *Some monoapparitic fourth order linear divisibility sequences*, Integers **12A** (2012), #A17.
39. H. C. Williams and R. K. Guy, *Odd and even divisibility sequences of order 4*, Integers **16** (2015), #A33.

Chapter 9
Prime Density of Companion Lucas Sequences

— *Which man first watched the moon?*
— *Which moon first lit the face of a man?* (Wang-Wei)

To be a great mathematician one must have the soul of a poet (Karl Weierstrass in a letter to Sofia Kovalevskaya)

It seems to me that the poet has to perceive that which others do not perceive, to look deeper than others look. And the mathematician must do the same thing (Sofia Kovalevskaya)

Abstract The central objective reason for this chapter is to show that the relative proportion, within the set of all primes, of primes which divide at least one term of a companion Lucas sequence can be computed precisely and unconditionally. For instance, we have known since Hasse that, on average, out of 24 primes, 17 divide some terms of the sequence $(2^n + 1)_{n\geq 0}$. Sections 9.1 and 9.2 are preliminary. Section 9.1 makes the word "proportion" precise, using density concepts. Section 9.2 mentions some of the rudiments of algebraic number theory necessary to state the classical density theorems for prime numbers, and, in particular, the celebrated theorem of Cebotarev[†]. Familiarity with abstract algebra, including rings, ideals, and quotient rings, and Galois theory is assumed. Section 9.3 applies the Cebotarev density theorem to a special class of recurrent sequences, the polynomial sequences $(P(n))_n$, where P is a monic polynomial in $\mathbb{Z}[x]$. This section can be skipped without

[†] The usual English spelling of this Russian surname is "Chebotarev," but sometimes "Tchebotaref," and its spelling varies a great deal in Western languages, even though they use the same Roman alphabet; thus, we prefer the simpler "Cebotarev," which at least contains the same number of letters as its cyrillic counterpart.

© Springer Nature Switzerland AG 2023

C. J.-C. Ballot, H. C. Williams, *The Lucas Sequences*, CMS/CAIMS Books in Mathematics 8, https://doi.org/10.1007/978-3-031-37238-4_9

any hindrance to reading the rest of the chapter. The early inquiries and works that later led Hasse to find a complete answer to the density of primes that divide companion Lucas sequences of the type $(a^n+1)_n$, a a square-free integer, are discussed in Sect. 9.4. The method of Hasse, and of Lagarias, who expanded the method of Hasse to some special second-order linear recurrences with irrational roots is presented in Sect. 9.5. In Sect. 9.6, we look at these prime density questions heuristically. The heuristics do not use the density theorems of algebraic number theory, save the Dirichlet density theorem, and, with simple tools, often permit an intuitive insight into these densities. The creative works of Laxton, who discovered a group structure for second-order recurrences that share the same characteristic polynomial, a group relevant to divisibility by primes, and extensions of this group to higher-order recurrences, are the object of Sect. 9.7. For m-th order linear recurrences, $m \geq 3$, we say, after Ward, that a prime is a maximal divisor of the sequence, when it divides $m-1$ consecutive terms of the recurrence. Section 9.8 shows how both the method of Hasse and Lagarias, and the aforementioned heuristics, apply, in some special instances, to the calculation of the prime density of maximal divisors of some linear recurrences. The final section reports about a foray made into the parallel world of polynomials over finite fields. The density of monic irreducible polynomials that divide the polynomial companion Lucas sequence $(X^n+1)_n$ is investigated.

9.1 How Do We Measure the Size of a Set of Primes?

Let $(p_n)_{n\geq 1}$ denote the sequence of rational prime numbers, where primes are ordered according to size, i.e., p_{n+1} is the least prime larger than p_n. The first few terms of the sequence are $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, and $p_5 = 11$. We denote the set of all primes $\{p_n;\ n \geq 1\}$ by $\mathcal{P}$. As is usual, the counting function for the number of primes not exceeding some positive real number x is denoted by $\pi(x)$. For instance, $\pi(10) = 4$. The prime number theorem (PNT) conjectured by Gauss in his teen years in the late eighteenth century and proved independently and in the same year, 1896, by Hadamard and de la Vallée Poussin, says that $\pi(x)$ is asymptotically equivalent to $x/\log x$ as x tends to infinity, where log is the Naperian or natural logarithm. The PNT is equivalent to the statement that $p_n \sim n \log n$, as n tends to infinity. (Indeed, $n = \pi(p_n) \sim p_n/\log(p_n)$ by the PNT. Hence, $p_n \sim n \log p_n$. Since p_n tends to infinity, the logarithms of p_n and of $n \log p_n$ must be asymptotically equivalent. Since $\log\log p_n = o(\log p_n)$, we get that $\log p_n \sim \log n$, as $n \to \infty$. This yields $p_n \sim n \log n$. For the converse, we obtain that $p_n \sim p_{n+1}$, $\log p_{n+1} \sim \log p_n \sim \log n$. Thus, if $p_n \leq x < p_{n+1}$, then $\pi(x) = n$ and $x/\log x \sim p_n/\log p_n \sim n \log n/\log n = n$.)

We denote the cardinality of a finite set A, i.e., the number of elements in A, either by $|A|$ or $\#A$. If $x > 0$ and S is a subset of $\mathcal{P}$, then $S(x)$ is the set of primes in S that do not exceed x. Thus, $\#S(x)$ is the number of

primes in $S(x)$. Finding out whether a set of primes, S, is finite or infinite is often a first step toward measuring the size of S. It can be a very difficult problem: to date we have not found a proof of the infinitude of the twin prime set in spite of all the heuristic and numeric evidence. But if we know S to be infinite, then seeking bounds, or better asymptotics, for the counting function $\#S(x)$ is the next step, or else determining whether S possesses a density relative to the set $\mathcal{P}$. If w is a function from $\mathcal{P}$ to the nonnegative real numbers such that $\sum_{p\in\mathcal{P}} w(p)$ diverges, then w is a weight function to which we may associate a density d_w: a subset S of $\mathcal{P}$ is said to possess a d_w-density, $d = d_w(S)$ ($d \in [0,1]$), if and only if

$$d = \lim_{x\to\infty} \frac{\sum_{p\in S(x)} w(p)}{\sum_{p\le x} w(p)}. \tag{9.1}$$

There are a few general consequences of this definition. A finite subset always has a zero d_w-density. Also, the d_w-densities are finitely additive, i.e., a finite disjoint union $\cup_{i=1}^{n} A_i$ of subsets of $\mathcal{P}$, each of which possesses a d_w-density, has a d_w-density equal to the sum $\sum_{i=1}^{n} d_w(A_i)$. Hence, adding or removing finitely many primes from a given set does not alter its d_w density. However, d_w-densities are not countably additive since $d_w(\mathcal{P}) = 1$, $\mathcal{P} = \cup_{i\ge1}\{p_i\}$ and $\sum_{i\ge1} d_w(\{p_i\}) = \sum_{i\ge1} 0 = 0$. These few properties are often expected to hold for any density concept whether the density is defined as in (9.1) or differently.

We present next the three most common densities used in relation to sets of rational primes, i.e., the natural, the analytic, and the logarithmic densities.

The *natural or asymptotic density* of a subset S of $\mathcal{P}$ (i.e., the natural or asymptotic density of S within the set of primes) is defined in analogy with the notion of natural density for subsets of the natural numbers (see Sect. 5.5.4). The set S has a natural density $d \in [0,1]$ if and only if the limit

$$\lim_{x\to\infty} \frac{\#S(x)}{\pi(x)}$$

exists and equals d. This corresponds to using the constant weightfunction $w(p) = 1$, p prime, in (9.1).

Upper and lower asymptotic densities are defined as the upper and lower limits of the function, respectively: $x \mapsto \frac{\#S(x)}{\pi(x)}$, as x tends to infinity. Such densities exist for all subsets of $\mathcal{P}$. (They are not in general finitely additive.) A set has an asymptotic density if and only if its upper and lower asymptotic densities coincide.

The *analytic or Dirichlet density* of $S \subset \mathcal{P}$ is defined as

$$\lim_{s\to1^+} \frac{\sum_{p\in S} 1/p^s}{\sum_{p\in\mathcal{P}} 1/p^s}, \tag{9.2}$$

if the limit exists.

As is well known, Euler showed the divergence of the series $\sum_n \frac{1}{p_n}$. More precisely, we have:

$$\sum_{p \le x} \frac{1}{p} \sim \log\log x, \qquad (p \in \mathcal{P}) \tag{9.3}$$

as x goes to infinity; see for instance [4, Thm. 4.12]. But if $s > 1$ is a real number and $x_n = 1/p_n^s$, then the series $\sum_{n\ge1} x_n$ converges. Indeed, the series $\sum_{n\ge1} x_n$ converges iff, by the PNT, $\sum_{n\ge3} 1/(n\log n)^s$ converges. But the latter series is dominated by the convergent Riemann series $\sum_n 1/n^s$. Thus, the expression $\big(\sum_{p\in S} 1/p^s\big)/\big(\sum_{p\in\mathcal{P}} 1/p^s\big)$ in (9.2) is well defined for all $s > 1$.

As turns out [11, Sect. 2], analytic density for a set of primes is equivalent to another useful density: the *logarithmic density*. A subset S of $\mathcal{P}$ possesses a logarithmic density $\delta = \delta(S)$ if and only if the limit

$$\lim_{x\to\infty} \frac{\sum_{p\in S(x)} 1/p}{\log\log x}$$

exists and equals δ. Thus, by (9.3), logarithmic density corresponds to using the weight function $w(p) = 1/p$ in (9.1).

If a set of prime numbers possesses a natural density d, then it must have a logarithmic density δ with $\delta = d$. The converse is false. There are sets of primes with a logarithmic density, but with no natural density. For instance, the set D_1 of prime numbers whose decimal expansion begins with the digit 1, i.e., $D_1 = \{11, 13, 17, 19, 101, 103, 107, 109, 113, 127, \ldots, 199, 1009, \ldots\}$ does not have a natural density: the upper and lower asymptotic densities of D_1 are distinct and can be calculated using the PNT. They are 5/9 and 1/9, respectively. But the logarithmic density of D_1 exists. Its value is $\delta(D_1) = \log_{10} 2 \simeq 0.301$. The set of natural numbers with first digit 1 is easily seen not to have an asymptotic density within the positive integers and, also, to possess upper and lower asymptotic densities of 5/9 and 1/9 as well as a logarithmic density equal to $\log_{10} 2$. General conditions were given [27] on subsets of the natural numbers, which include the subset of prime numbers, for the natural and logarithmic densities to be preserved when conditioning with respect to such subsets.

More generally, $\delta(D_k) = \log_{10}(1 + 1/k)$, where D_k is the set of prime numbers whose first decimal digit is k, $1 \le k \le 9$. (Some readers may recognize the exact frequency given by Benford's law. However, Benford's law stipulates that many lists of numbers obey this frequency with respect to asymptotic density.[†] In the present case, this frequency only holds with re-

[†] If you have the patience, go to your favorite supermarket (Carrefour, Loblaw Companies, Safeway, etc.) and write down the first nonzero digit for the prices of some 400 items. You should get fairly close to $\log_{10}(1 + 1/k)$ for the proportion of digit k. Note that $\sum_{k=1}^{9} \log_{10}(1 + 1/k) = 1$. Or make a list of all rivers in Russia, or in Canada, and mark the first digit of the lengths of these rivers and again the frequency of digit k should get near $\log_{10}(1+1/k)$, no matter whether length is measured in miles or kilometers. We refer

spect to logarithmic density; one says that prime numbers obey the weak Benford law.)

There is an ordering on densities. We say that $d_1 \preceq d_2$ if and only if, for all subsets S of $\mathcal{P}$, the existence of $d_2(S)$ implies the existence of $d_1(S)$ and $d_1(S) = d_2(S)$. For example, from what we said above, $\delta \preceq d$. Two densities d_1 and d_2 are *equivalent* if and only if $d_1 \preceq d_2$ and $d_2 \preceq d_1$. This equivalence relation is denoted by $\sim$. Thus, $\delta \sim d_A$, if d_A is the analytic density defined in (9.2). If $d_1 \preceq d_2$ and $d_1 \not\sim d_2$, then we write $d_1 \prec d_2$. Murata [49, 50] showed that the densities $d_{\alpha,\beta} := d_{f_{\alpha,\beta}}$, where the weight functions $f_{\alpha,\beta}$, $\alpha \geq 0$, $\beta \geq 0$ are defined by

$$f_{\alpha,\beta}(x) = x^{\alpha-1}(\log x)^{\beta},$$

give rise to exactly three distinct equivalence classes of densities. The natural density $d = d_{1,0}$ is equivalent to $d_{\alpha,\beta}$ for all $\alpha > 0$ and $\beta \geq 0$. The logarithmic density $\delta = d_{0,0}$ stands alone in its equivalence class. The third class contains the density $d_{0,1}$ and comprises all remaining densities $d_{\alpha,\beta}$ with $\alpha = 0$ and $\beta > 0$. Murata [50] showed that the ordering

$$\delta \prec d_{0,1} \prec d_{1,0},$$

holds.

9.2 The Classic Density Theorems

There are at least four main density theorems of historic importance: the Dirichlet, the Kronecker-Frobenius, the Frobenius , and the Cebotarev density theorems. The Cebotarev theorem actually subsumes the other theorems. Kronecker and Frobenius discovered their theorems in the early 1880s. We make mention of the Dirichlet theorem first. For the sake of brevity, we will not state the Frobenius theorem. The Cebotarev theorem, proved in 1922 and published in 1925 [73], had been an early conjecture of Frobenius. In fact, the Frobenius theorem, although weaker than Cebotarev's, often suffices in many applications. The statements of the two theorems are close relatives; one obtains Cebotarev's from the statement of the Frobenius theorem on replacing division classes by conjugacy classes, where division classes come from a slightly weaker relation than conjugacy for group elements. Cebotarev [68] claimed to have found a proof of his theorem while carrying water uphill and buckets of cabbage downtown, not in the cozyness of an office.

---

the reader interested in Benford's law to the book [19], or the survey paper [18] by the same two researchers, and to [36, Chap. 1] for an excellent intuitive general-public presentation of the Benford phenomenon.

If a, b are coprime positive integers, Dirichlet proved in 1837 that the set of primes of the form $ax + b$, where x is an integer, is infinite. In fact, it has Dirichlet density $\delta = 1/\varphi(a)$. With the analytic methods that accompanied the proofs of the PNT in 1896, it was possible to show this set has natural density $d\ (= 1/\varphi(a))$.[†] The only arithmetic progressions $ax+b$, with common difference a, which contain infinitely many primes require $\gcd(a, b) = 1$. Thus, we see that primes are equidistributed among the $\varphi(a)$ distinct progressions $\{ax + b\}$, $1 \le b \le a$, $\gcd(a, b) = 1$, at least in density terms. See [29] for a more precise discussion in particular when $a = 4$ and b is either 1 or 3. Thus, the statement of the Dirichlet theorem for primes in arithmetic progressions often includes the density result, i.e., if $\gcd(a, b) = 1$, then

$$d(\pi_{a,b}) = \delta(\pi_{a,b}) = 1/\varphi(a), \tag{9.4}$$

where $\pi_{a,b}$ is the set of primes of the form $ax + b$.

Remark 41 The density theorems of Dirichlet, Kronecker, Frobenius, and Cebotarev were first established in relation to analytic density. It was later shown any set of primes which possesses a density from one of these theorems must have a natural density as well. See the remarks of Serre [61, Chap. VI], and for proofs [55, Chap. 5] and [51, Theorem 7.10*], for instance.

We note in passing that the set of primes with first decimal digit 1 cannot be described using the Cebotarev theorem. As mentioned in Sect. 9.1, this set has logarithmic (hence, analytic density), but no natural density.

We state a few basic facts about number fields which are part of introductory books on algebraic number theory; see, e.g., [1, 40, 53].

A *number field* is a subfield of the field $\mathbb{C}$ of complex numbers which, as a vector space over the field of rational numbers $\mathbb{Q}$, is of finite dimension. Therefore, all numbers in a number field are algebraic: they are the zeros of some polynomial over $\mathbb{Z}$. Those that are zeros of monic polynomials over $\mathbb{Z}$ are called *algebraic integers*. Algebraic integers in a number field K form a ring $\mathcal{O}_K$. Thus, $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. Also, for example, $\mathbb{Q}(\sqrt{2})$, the field extension of $\mathbb{Q}$ generated by $\sqrt{2}$, is $\{r + s\sqrt{2};\ r, s \in \mathbb{Q}\}$. That is, $\{1, \sqrt{2}\}$ is a finite basis of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. Its ring of integers is $\{r + s\sqrt{2};\ r, s \in \mathbb{Z}\}$. However, the ring of integers of $\mathbb{Q}(\sqrt{5})$ is $\{r + s\alpha;\ r, s \in \mathbb{Z}\}$, where α is $(1 + \sqrt{5})/2$. The ring of algebraic integers $\mathcal{O}_K$ of a number field K has the property that every prime ideal is a maximal ideal. Moreover, unique factorization of rational integers into their prime factors has a generalization in a ring $\mathcal{O}_K$: every ideal factorizes uniquely into prime ideals. Rings of integers, unlike $\mathbb{Z}$, are

[†] The Dirichlet density theorem stated in the form

$$|\{p \le x;\ p \equiv b \pmod a\}| = \frac{1}{\varphi(a)} \int_2^x \frac{dt}{\log t} + O_a(xe^{-c\sqrt{\log x}}),$$

for some positive c independent of a, is often called the PNT for arithmetic progressions.

not in general principal ideal domains. But any ideal I in $\mathcal{O}_K$ may always be generated by two elements, i.e., there exist a and b in $\mathcal{O}_K$ such that $I = (a, b)$. A prime ideal P in $\mathcal{O}_K$ contains a (unique) rational prime p. The finite field $\mathcal{O}_K/P$ is a field extension of $\mathbb{Z}_p := \mathbb{Z}/(p)$. Its degree $f = f(P|p)$ is called the *inertial degree* of P over p. Thus, $(\mathcal{O}_K/P)/\mathbb{Z}_p$ is isomorphic to the finite Galois field $GF(p^f)$. The corresponding Galois group of the finite field extension is cyclic of order f generated by the *Frobenius map* σ_p: $x \mapsto x^p$. Suppose L/K is a number field extension, i.e., L is a number field containing K. Then, there exists an algebraic number a, called a *primitive element* of L/K, such that $L = K(a)$, where $K(a)$ is the smallest number field containing K and a. In fact, a can be chosen to be an algebraic integer. The ideal (p) generated by a rational prime in the ring $\mathcal{O}_K$ of a number field K need not remain a prime ideal. Say

$$(p) = P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r}, \tag{9.5}$$

is the prime ideal factorization of (p) in $\mathcal{O}_K$, i.e., the P_i's are prime ideals in $\mathcal{O}_K$ and the e_i's are positive integers. Then, we say that p *splits into* r primes in K and e_i is the *ramification index* of P_i over p. A prime p is said to be ramified in K if at least one of the e_i's is greater than 1. Since only finitely many primes are ramified in a given number field K, we state our theorems in the unramified case for, as, was remarked in Sect. 9.1, removing finitely many primes does not alter densities. Suppose the degree $[K : \mathbb{Q}]$, i.e., the dimension of K as a vector space over $\mathbb{Q}$, is n. If f_i is the inertial degree of P_i over p, $i = 1, \ldots, r$, in (9.5), then we must have:

$$n = \sum_{i=1}^{r} e_i f_i, \tag{9.6}$$

or, in the unramified case, $\sum_{i=1}^{r} f_i = n$. We say the prime p *splits completely* in K whenever all inertial degrees f_i are 1, i.e., when $r = n$. The prime p is *inert* if the ideal (p) remains prime in $\mathcal{O}_K$, i.e., if $r = 1$ and $f = f((p)|p) = n$.

Suppose L/K is a Galois number field extension, i.e., all field embeddings of L in $\mathbb{C}$ which fix K pointwise are automorphisms of L. Put $G = \mathrm{Gal}(L/K)$. Suppose P is a prime ideal in $\mathcal{O}_K$, unramified in L, and Q is a prime ideal in $\mathcal{O}_L$ above P, i.e., such that Q contains P, or equivalently, such that Q is a prime ideal factor of $P\mathcal{O}_L$. Note that the extension $(\mathcal{O}_L/Q)/(\mathcal{O}_K/P)$ may be seen as a finite field extension.[†] The group G acts transitively on the prime ideal factors of the ideal $P\mathcal{O}_L$. The *decomposition group* $D = D(Q|P)$ is the stabilizer of Q in this action, i.e., for $\sigma \in G$, we have $\sigma \in D$ if and only if $\sigma(Q) = Q$. If $\sigma \in D$, then σ induces an automorphism of the finite field extension $(\mathcal{O}_L/Q)/(\mathcal{O}_K/P)$. In fact, D is isomorphic to the cyclic Galois group $\bar{D}$ of this finite field extension. (The group $\bar{D}$ has for generator the (generalized) Frobenius map σ_P: $x \mapsto x^{|P|}$, where $|P|$ is $p^{f(P|p)}$, p being the

[†] Since $P = Q \cap \mathcal{O}_K$, P is the kernel of the map: $\mathcal{O}_K \mapsto \mathcal{O}_L/Q$ which sends x to $x + Q$; thus, $\mathcal{O}_K/P$ is injected into $\mathcal{O}_L/Q$ which contains an isomorphic image of $\mathcal{O}_K/P$.

rational prime under P.) The corresponding generator $\Phi = \Phi(Q|P)$ of the group D is called the *Frobenius automorphism* relative to P and Q. It has the defining property that for all $x \in \mathcal{O}_L$

$$\Phi(x) \equiv x^{|P|} \pmod{Q}, \tag{9.7}$$

i.e., Φ is the only element of G with property (9.7). We readily see that if $\sigma \in G$, then $\Phi(\sigma(Q)|P) = \sigma\Phi\sigma^{-1}$. Thus, in a normal extension, the prime ideals above P all have the same inertial degree f, and the degree of the Galois extension is rf, if P splits into r primes. Note that as we shift from one prime ideal above P to another, the Frobenius automorphism visits a whole conjugacy class, $C_P = C_P(L/K)$, of G. This conjugacy class is usually denoted by the Artin symbol

$$\left[\frac{L/K}{P}\right].$$

We are ready to state the Cebotarev theorem. We do so restrictively by assuming the bottom field is $\mathbb{Q}$ since we are interested in the natural density of rational primes rather than the Dirichlet density of prime ideals in a general number ring $\mathcal{O}_K$. The theorem asserts that, as we go through primes, the frequency with which the Frobenius automorphism Φ belongs to a given conjugacy class C of the Galois group G is proportional to the size of C, i.e., is equal to the ratio $|C|/|G|$.

Theorem 127 (Cebotarev's density theorem) *Let K be a Galois number field extension of the rationals with Galois group G. Let C be a conjugacy class of G. Then, the set of unramified primes p in K for which $C_p(K/\mathbb{Q})$ is C has a Dirichlet and a natural density equal to $|C|/|G|$.*

We state the Kronecker-Frobenius density theorem, an immediate and useful corollary to the Cebotarev theorem.

Theorem 128 (The Kronecker-Frobenius density theorem) *Let K be a Galois number field extension of the rationals with Galois group G. Then, the set of rational primes which split completely in K has a natural density equal to $1/|G|$.*

Proof If a rational prime p splits completely in $\mathcal{O}_K$, then the inertial degree of a prime P in K above p is 1. Thus, the Frobenius automorphism $\Phi(P|p)$ has order 1 in G. The identity of the Galois group forms a conjugacy class all by itself. The result follows from the Cebotarev theorem. □

We state another corollary for cyclotomic extensions. It shows how the Dirichlet density theorem follows from the Cebotarev density theorem.

Corollary 129 Suppose K is the cyclotomic Galois extension $\mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/n}$, $n \geq 1$ an integer. Then, primes of the form $k + nx$, $(x \geq 0)$, where $1 \leq k \leq n$, $\gcd(k, n) = 1$, have Frobenius automorphism defined by $\zeta \mapsto \zeta^k$. Their density is $1/\varphi(n)$. □

Proof The Galois group G of $\mathbb{Q}(\zeta)$ is the set of automorphisms of K defined by $\tau_k : \zeta \mapsto \zeta^k$, for $1 \leq k \leq n$ and $\gcd(k, n) = 1$. Thus, G is isomorphic to the multiplicative group of integer modulo n, and $|G| = \varphi(n)$. The automorphism that sends ζ to ζ^p, i.e., τ_p, satisfies the property (9.7). Therefore, τ_p is the Frobenius automorphism $\Phi(P \,|\, p)$, (P in $\mathcal{O}_K$ above p). Since $\zeta^k = \zeta^p$ if and only if $p \equiv k \pmod{n}$, we see that $\Phi(P \,|\, p) = \tau_k$ if and only if p has the shape $k + nx$. Since G is abelian, $\{\tau_k\}$ is a conjugacy class of G. Thus, by Cebotarev theorem, primes of the form $k + nx$ have density $1/\varphi(n)$. □

Remark 42 Note that the order f of $\Phi(P|p)$, P a prime ideal in $\mathcal{O}_K$, is equal to the multiplicative order of p modulo n. Hence, primes in the progression $k + nx$ split into $r = \varphi(n)/f$ prime ideals in $\mathcal{O}_K$. In particular, primes of the form $1 + nx$ split completely in K, while those of the form $-1 + nx$, $(n > 2)$, split into $\varphi(n)/2$ prime ideals in $\mathcal{O}_K$.

Although not a density theorem, the Kummer-Dedekind theorem is often useful in our context. It points to a complete analogy between two factorizations: the factorization of an irreducible polynomial modulo a prime ideal and the factorization of this prime ideal in an extension containing a zero of the polynomial. See, e.g., [40, Theorem 27] for a proof.

Theorem 130 (The Kummer-Dedekind theorem) *Suppose L/K is an extension of number fields and α is an algebraic integer such that $L = K(\alpha)$. Let $m = m_\alpha(x)$ denote the minimal polynomial of α over $\mathcal{O}_K$. Then, for all but finitely many prime ideals P in $\mathcal{O}_K$, the factorization of $m \pmod{P}$ has the shape:*

$$m = m_1 m_2 \cdots m_r \pmod{P} \iff P\mathcal{O}_L = Q_1 Q_2 \cdots Q_r,$$

where Q_i is the prime ideal $P\mathcal{O}_L + (m_i(\alpha))$ in $\mathcal{O}_L$ lying above P.

Thus, if $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$, $(i = \sqrt{-1})$, then odd rational primes p which split into two ideals in $\mathcal{O}_L$ are the primes $1 \pmod 4$. Indeed, the minimal polynomial of i, $m_i(x) = x^2 + 1$, factorizes modulo p into two linear factors if and only if -1 is a square modulo p, i.e., if $p \equiv 1 \pmod 4$. Primes of the form $3 + 4k$ are inert primes. Say $p = 5$. Then, $x^2 + 1 = x^2 - 4 = (x - 2)(x + 2) \pmod p$. By Theorem 130, the two prime ideals above 5 in $\mathcal{O}_L$ are $P_1 = (i - 2, 5)$ and $P_2 = (i + 2, 5)$. Since $5 = (2 - i)(2 + i)$, 5 belongs to the ideals $(2 - i)$ and $(2 + i)$. Hence, $P_1 = (2 - i)$ and $P_2 = (2 + i)$. More generally, for all primes $p \equiv 1 \pmod 4$, say $p = u^2 + v^2$, the two prime ideals above p are the principal ideals $(u - iv)$ and $(u + iv)$. Here, $\mathcal{O}_L$ is the ring of Gaussian integers $\mathbb{Z}[i]$, which is well known to be a principal ideal domain.

9.3 Polynomial Modulo p and Cebotarev

The Galois group of a polynomial $f \in \mathbb{Z}[x]$ is the Galois group of $L/\mathbb{Q}$, where L is the splitting field of f. That is, L is the number field extension of $\mathbb{Q}$ generated by the zeros of f. If f is irreducible of degree $n \geq 1$, then G may be viewed as a transitive subgroup of the symmetric group S_n. Indeed, G acts transitively on the zeros $\alpha_1, \alpha_2, \ldots, \alpha_n$ of f. In fact, in some sense, for almost all degree-n irreducible polynomials over $\mathbb{Z}$, G is isomorphic to S_n [28].

Let us assume, for the sake of simplicity, that α is an algebraic integer of degree n, i.e., its monic minimal polynomial $m = m_\alpha(x)$ over $\mathbb{Z}$ has degree n. Denote $\mathbb{Q}(\alpha)$ by K and the splitting field of $m_\alpha(x)$ by L. Let G be the Galois group of the normal extension $L/\mathbb{Q}$ and H the subgroup of G of automorphisms that fix K pointwise, or equivalently that fix α. Thus, H is the Galois group of L/K, and the index of H in G, $[G : H]$, is equal to $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$ by Galois theory. The Kummer-Dedekind theorem (Theorem 130) establishes a one-to-one correspondence between the factorization of m into r irreducible factors modulo p and the splitting type of the ideal (p) in $\mathcal{O}_K$ into r prime ideals, where degrees of the factors of m match the inertial degrees of corresponding prime ideals. This same common factorization can be expressed in yet another way: the action of the Frobenius automorphism $\Phi = \Phi(Q \,|\, p)$, where Q is a prime ideal above p in $\mathcal{O}_L$, it does not matter which such Q, on the complex zeros of $m_\alpha(x)$, yields a permutation in S_n whose cycle-type decomposition matches the factorization of m modulo p. More precisely, we have, using the above notation, the following theorem.

Theorem 131 *For all but finitely many primes p, except primes ramified in L or divisors of the discriminant of $m_\alpha(x)$, $m_\alpha(x)$ splits into r irreducible factors of degrees $f_1 \leq f_2 \leq \cdots \leq f_r$ in $\mathbb{F}_p[x]$ if and only if the decomposition of $\Phi(Q \,|\, p)$ into disjoint cycles as a permutation of the complex zeros of $m_\alpha(x)$ contains r cycles of respective lengths $f_1, f_2, \ldots, f_r$, where Q is any prime ideal of $\mathcal{O}_L$ above p.*

Proof The action of $\Phi = \Phi(Q \,|\, p)$ on the left cosets σH of H in G by left multiplication produces r orbits whose lengths match the inertial degrees of the prime ideals P above p in $\mathcal{O}_K$ [40, Thm. 33]. The action is given by $\Phi \cdot \sigma H = \Phi\sigma H$. The orbits $\sigma H, \Phi\sigma H, \Phi^2\sigma H, \ldots, \Phi^{\ell-1}\sigma H$ are in one-to-one correspondence with the prime ideals $P = \sigma(Q) \cap \mathcal{O}_K$ which come into the factorization of $p\mathcal{O}_K$. Moreover, $\ell = f(P \,|\, p)$. To each such orbit corresponds a cycle in the action of Φ on the complex zeros of $m_\alpha(x)$, namely, the cycle $(\sigma(\alpha), \Phi(\sigma(\alpha)), \Phi^2(\sigma(\alpha)), \ldots, \Phi^{\ell-1}(\sigma(\alpha)))$ with $\Phi^\ell(\sigma(\alpha)) = \sigma(\alpha)$. □

The Cebotarev density theorem and Theorem 131 tell us how often a polynomial factorizes in a prescribed manner modulo primes. We indicate this in the form of an immediate corollary.

Corollary 132 Let $g(x)$ be a monic irreducible polynomial over $\mathbb{Z}$ with Galois group G. Suppose τ in G decomposes, as a permutation of the complex zeros of $g(x)$, into r cycles of lengths $f_1, f_2, \ldots, f_r$. Then, the set of rational primes such that $g(x)$ factorizes into r irreducible factors in $\mathbb{F}_p[x]$ of degrees $f_1, f_2, \ldots, f_r$ has a natural density equal to $|\mathcal{C}|/|G|$, where $\mathcal{C}$ is the conjugacy class of τ in G. □

Thus, the factorization of a polynomial modulo primes can be used to yield information on the Galois group of the polynomial, and determine its structure; see [75, Sect. 8.10].

Before examining a few density-related consequences on the factorization of polynomials modulo primes, we provide a couple of numerical tables which illustrate Corollary 132.

The polynomial $f(x) = x^4 - 4x^2 - x + 1$ in $\mathbb{Z}[x]$ has a Galois group G isomorphic to S_4. Therefore, all permutations of its four zeros occur. The first line of Table 9.1 indicates the five cycle-type decompositions of permutations in S_4. The second line gives the density of rational primes p for which the Frobenius map $\Phi(P\,|\,p)$ lands in the various conjugacy classes of G. Here, a conjugacy class is characterized by a cycle-type decomposition, and P is a prime above p in $\mathcal{O}_L$, L being the splitting field of $f(x)$. The next 3 lines indicate, for 3 lists of 24 consecutive primes p, how many achieve a given factorization type for $f(x) \pmod p$. Even on such a small sample of primes, we see a fair adequation of the number of primes such that $f(x)$ factorizes into a given type, say, for example, two linear factors and a quadratic, and the conjugacy class size of transpositions in S_4 which has type $[1, 1, 2]$. Line 5 has the number of expected primes if the density proportion were to be respected for each of lines 2, 3, and 4. The discriminant of $f(x)$ is $19 \cdot 103$. Thus, f has multiple zeros modulo the primes 19 and 103. More precisely, the factorization of f is of type $[1^2, 2]$ in both cases. They were assimilated as belonging to the type $[1, 1, 2]$. (Note that, among the first 72 primes, $f(x)$ factorizes into 4 linear factors only for $p_{69} = 347$, namely, $(x-117)(x-140)(x+106)(x+151) \pmod{347}$.)

Table 9.1 Factorization of $x^4 - 4x^2 - x + 1 \pmod p$

Cycle types	$[1,1,1,1]$	$[1,1,2]$	$[2,2]$	$[1,3]$	$[4]$
Densities	1/24	1/4	1/8	1/3	1/4
$p_1, \ldots, p_{24}$	0	5	1	11	7
$p_{25}, \ldots, p_{48}$	0	6	3	10	5
$p_{49}, \ldots, p_{72}$	1	5	4	8	6
'Expected numbers'	1	6	3	8	6
$p_1, \ldots, p_{72}$	1	16	8	29	18
'Expected numbers'	3	18	9	24	18

Let us consider the polynomial $g(x) = x^4 - 2$. The decomposition field of g is $\mathbb{Q}(\sqrt[4]{2}, i)$, where $i = \sqrt{-1}$. Put $\alpha = \sqrt[4]{2}$. The four zeros of g are α, αi, $-\alpha$, and $-\alpha i$. Let us number them as 1, 2, 3, and 4, respectively. The Galois group is of order 8, and because a member of G has to send i to $\pm i$ and α to $\pm\alpha$ or $\pm\alpha i$, one easily verifies that G is isomorphic to the dihedral group generated by complex conjugation $\tau = (24)$ and $\sigma = (1234)$. Thus, G contains the identity, two transpositions (13) and τ, the three permutations of type $[2, 2]$, and two 4-cycles σ and σ^{-1}. Since the discriminant of g is a power of 2, we tested the factorization of g modulo all 24 odd primes less than 100 and recorded the data in the table below.

Table 9.2 Factorization of $x^4 - 2 \pmod{p}$

Cycle types	$[1, 1, 1, 1]$	$[1, 1, 2]$	$[2, 2]$	$[4]$
Densities	1/8	1/4	3/8	1/4
$p_2, \ldots, p_{25}$	2	6	10	6
"Expected numbers"	3	6	9	6

We turn our attention to the following question. How many zeros should we expect an irreducible polynomial over the integers to possess in $\mathbb{Z}_p[x]$, where p is a prime? Say $f(x)$ is an irreducible polynomial of positive degree n over $\mathbb{Z}$. If $0 \le i \le n$, then the set of primes p such that $f(x)$ has exactly i zeros modulo p has a density, say d_i, as we will see. We have the obvious relationship $\sum_{i=0}^{n} d_i = 1$. Furthermore, the average number of zeros of f modulo p as p varies through the primes is 1.

More formally, we have the following.

Theorem 133 *Let $f(x)$ be an irreducible polynomial over $\mathbb{Z}$ of degree $n \ge 1$. Let d_i, $0 \le i \le n$, denote the density of the set of primes p for which f modulo p has exactly i zeros. Then,*

$$\sum_{i=1}^{n} i d_i = 1.$$

Theorem 133 was first stated by Kronecker [34], but a complete proof that included the existence of the densities d_i came with Frobenius.

For instance, if $f(x) = x^2 + 1$, then $d_1 = 0$ since f cannot have a zero without having two. Thus, $2d_2 = 1$. Therefore, $d_0 = d_2 = 1/2$. That is, primes congruent to 1 (mod 4) have the same density as those -1 (mod 4), something we already knew from the Dirichlet theorem (9.4). Say f is a cubic polynomial with alternating Galois group A_3. Only the identity of A_3 has some fixed point. It fixes the three zeros. By the Cebotarev theorem, the density of primes for which the Frobenius automorphism is the identity is 1/3. Hence, we see that $d_3 = 1/3$, $d_1 = d_2 = 0$ and $d_0 = 2/3$. Thus, we have checked that Theorem 133 holds in such a case. If the Galois group is

S_3, then by the Cebotarev density theorem $d_3 = 1/6$, $d_1 = 1/2$, since S_3 contains three transpositions, and $d_0 = 1/3$ (there are two three-cycles, or $d_0 + d_1 + d_3 = 1$). We have again verified that $3d_3 + d_1 = 1$.

Theorem 133 can easily be extended further. Suppose f is a nonzero discriminant polynomial over $\mathbb{Z}$. Then, f has N irreducible factors in $\mathbb{Q}[x]$ if and only if

$$\sum_{i=1}^{n} id_i = N.$$

Remark 43 Because of the rapidity with which counts of primes experimentally settle down toward the actual densities, this property could possibly be used to determine N.

We establish a couple of lemmas before proving Theorem 133. The first lemma was proved by Frobenius in 1887, but its genesis originated in a work of Cauchy in 1845 according to Rotman [58, Thm. 3.26].

Lemma 34 *Suppose G is a finite group acting on a finite set X. Then,*

$$N = \frac{1}{|G|} \sum_{g \in G} F(g),$$

where N is the number of orbits in the action and $F(g)$ is the number of elements in X that are fixed by g.

Proof If x and y are in the same orbit O, their respective stabilizers S_x and S_y in G have the same cardinality, say S_O. Indeed, if $\sigma(x) = y$ for some $\sigma \in G$, then $S_x = \sigma^{-1} S_y \sigma$. The cosets of S_x are naturally in one-to-one correspondence with the elements of O. Thus, $|G| = |S_x| \cdot [G : S_x] = S_O \cdot |O|$. Therefore,

$$\begin{aligned}
\sum_{g \in G} F(g) &= \sum_{g \in G} \sum_{x \in X} [\, g \cdot x = x \,] = \sum_{x \in X} \sum_{g \in G} [\, g \cdot x = x \,] \\
&= \sum_{x \in X} |S_x| = \sum_{\text{orbits } O} \sum_{x \in O} |S_x| = \sum_{\text{orbits } O} |O| \cdot S_O \\
&= \sum_{\text{orbits } O} |G| = N \cdot |G|,
\end{aligned}$$

where we have used the Iverson symbol $[-]$. □

Lemma 35 *Let f be an irreducible polynomial over $\mathbb{Z}$ with n complex zeros, $(n \geq 1)$, and Galois group G. Let Z_i, $i = 0, \ldots, n$, be the set of elements of G which fix exactly i zeros of f. Then, the primes p for which f has i zeros in its factorization modulo p have a natural density $d_i = |Z_i|/|G|$.*

Proof Viewing G as a transitive subgroup of the symmetric group S_n, we see that Z_i is a union of conjugacy classes, since two elements in the same conjugacy class must have the same cycle-type decomposition and, in particular, the same number of fixed points. Hence, by Corollary 132, the set of primes p for which the factorization of f modulo p has i linear factors has density $|Z_i|/|G|$. □

Proof of Theorem 133. By Lemma 34, we find that

$$|G| = \sum_{g\in G} F(g) = \sum_{i=0}^{n} \sum_{g\in Z_i} F(g)$$
$$= \sum_{i=0}^{n} \sum_{g\in Z_i} i = \sum_{i=0}^{n} i|Z_i|.$$

Hence, by Lemma 35,

$$1 = \sum_{i=0}^{n} i\frac{|Z_i|}{|G|} = \sum_{i=0}^{n} id_i.$$

Theorem 134 *Suppose $f(x)$ is an irreducible monic polynomial over $\mathbb{Z}$. Let α be a zero of $f(x)$, $K = \mathbb{Q}(\alpha)$ and L be the splitting field of $f(x)$ in $\mathbb{C}$. Let G be the Galois group of $L/\mathbb{Q}$ and H be the subgroup of the automorphisms of G which fix K pointwise. Then, the density d of primes p for which $f(x)$ has at least one linear factor modulo p is given by*

$$d = \frac{|\cup_{\sigma\in G} \sigma^{-1}H\sigma|}{|G|}.$$

Proof If $\sigma \in G$, then $\sigma H\sigma^{-1}$ is the subgroup of G which fixes $\sigma(\alpha)$. Since G permutes transitively the zeros of $f(x)$, the set $\cup_{\sigma\in G}\sigma H\sigma^{-1}$ consists of all the elements of G which have at least one fixed point. Noting that $\cup_{\sigma\in G}\sigma H\sigma^{-1}$ is a union of conjugacy classes, namely, of the conjugacy classes containing an element of H, we see, by Corollary 132, that $|\cup_{\sigma\in G}\sigma^{-1}H\sigma|/|G|$ is the density of primes for which $f(x)$ has at least one linear factor in its factorisation modulo p. □

It is well known that the proportion of permutations with no fixed points in S_n approaches e^{-1} as n tends to infinity. This gives the following corollary.

Corollary 135 Suppose $f(x)$ is an irreducible monic polynomial over $\mathbb{Z}$ of degree n with Galois group isomorphic to S_n. Then, the set of primes p such that $p \mid f(k)$, for some integer k, possesses the prime density:

$$d_f = 1 - \sum_{k=0}^{n} \frac{(-1)^k}{k!},$$

which tends to $1 - \frac{1}{e} \simeq 0.6321$ as n increases. □

Proof If G is isomorphic to S_n, then $\cup_{\sigma\in G}\sigma^{-1}H\sigma = \cup_{i=1}^{n} S_n(i)$, where $S_n(i)$ are the permutations of $\{1, 2, \ldots, n\}$ which fix i, $(1 \le i \le n)$. By the principle of inclusion-exclusion, we get:

$$\begin{aligned}|\cup_{i=1}^{n} S_n(i)| &= \sum_{1\le i\le n} |S_n(i)| - \sum_{1\le i<j\le n} |S_n(i)\cap S_n(j)| + \cdots \\ &= \binom{n}{1}|S_{n-1}| - \binom{n}{2}|S_{n-2}| + \cdots + (-1)^{n-2}\binom{n}{n-1}|S_1| \\ &\quad + (-1)^{n-1}.\end{aligned}$$

Hence, dividing by $n!$, we obtain:

$$\begin{aligned}d_f &= 1 - \frac{1}{2!} + \frac{1}{3!} - \cdots + \frac{(-1)^{n-1}}{n!} \\ &= 1 - \left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}\right) \\ &= 1 - \sum_{k=0}^{n} \frac{(-1)^k}{k!},\end{aligned}$$

from which the result follows. □

Examples. Suppose $f(x)$ is the polynomial $x^4 - 4x^2 - x + 1$ with Galois group S_4 of Table 9.1. By Corollary 135,

$$d_f = 1 - \left(1 - 1 + \frac{1}{2} - \frac{1}{6} + \frac{1}{24}\right) = \frac{5}{8} \simeq 0.625.$$

The density d_f is also the sum of the densities associated with each of the decomposition types $[1, 1, 1, 1]$, $[1, 1, 2]$, and $[1, 3]$, i.e., with those types which have at least one fixed point. By Table 9.1, this is the sum $\frac{1}{24} + \frac{6}{24} + \frac{8}{24}$. If $g(x)$ is the polynomial $x^4 - 2$ of Table 9.2 with dihedral Galois group G, then $H = \langle\tau\rangle$, where, recycling the notation adopted for the zeros of $g(x)$ above Table 9.2, $\tau = (24)$, i.e., τ is complex conjugation. The only conjugate of τ in G is (13). Thus, $\cup_{\sigma\in G}\sigma^{-1}H\sigma$ is made up of the identity and the two transpositions (24) and (13) giving a density $d_g = 3/8$.

Corollary 136 Suppose $f(x)$ is an irreducible monic polynomial over $\mathbb{Z}$ of degree n. Then, the set of primes p for which $p \nmid f(t)$ for all integers t has a density d_0 which satisfies

$$d_0 \ge \frac{n-1}{n!}.$$

Proof The condition $p \nmid f(t)$ for all integers t is equivalent to $f \pmod p$ having no zeros. Thus, this set has a density, denoted by d_0 in Theorem 133, by Lemma 35. Moreover, using Theorem 133 and its notation

$$0 = \sum_{i=1}^{n} id_i - \sum_{i=0}^{n} d_i \implies$$
$$d_0 = \sum_{i=1}^{n} (i-1)d_i \geq (n-1)d_n \geq \frac{n-1}{n!},$$

since, by Theorem 128, $d_n = 1/|G| \geq 1/n!$, where G is the Galois group of f. □

As a consequence if f is of degree $n \geq 2$, primes which do not divide any $f(t)$, (t an integer), have a positive density. Thus, if f has a zero modulo all but finitely many primes, f must be a linear polynomial. We point out that no elementary proof is known of the fact that infinitely many primes do not divide $f(t)$, for any t, when f is irreducible of degree ≥ 2 [47]. A contrario, there are several elementary proofs of the existence of infinitely many primes dividing a nonconstant polynomial in $\mathbb{Z}[x]$ (see, e.g., [40, Ex. 30, p. 91], [47]); several proofs are based on the rate of growth of polynomial sequences and the fact they take the same integer value at most d times, where d is the degree.

9.4 Initial Inquiries of Sierpiński, Brauer, and Ward

Given a sequence of rational integers $X = (X_n)_{n\geq 0}$ and a prime number p, we say that p divides X, or p is a divisor of X, and write $p \mid X$, to say that p is a factor of at least one term of X. There are relatively few sequences for which we know how to prove unconditionally, i.e., without additional conjectures such as Riemann hypotheses, the existence of a natural density for the set $\mathcal{P}(X)$ of prime divisors of X, and simultaneously compute its value. That is, if we discard trivial instances where that density is 0 or 1, e.g., a nonzero geometric sequence has a 0 density, while a sequence, periodic modulo primes, with a zero term, such as the Fibonacci sequence, has a 1 density. However, as seen in Sect. 9.3, and in Theorem 134, if X is a polynomial sequence, e.g., $X_n = n^2 + 1$, $n^4 - 2n^2 - n + 1$ or $n^4 - 2$, then we can find the exact *prime density* of X, i.e., of the set $\mathcal{P}(X)$, provided we are able to find the associated Galois group.

Even if early inquiries did not seek answers in density terms, estimating the size of the set of prime divisors of a companion Lucas sequence began with two independant sources, one in Europe with a paper of Sierpiński of 1958 followed by a 1960 paper of Brauer having to do with the sequence $(2^n + 1)$ and sequences $(a^n + 1)$, a a positive integer; the other source originated from California with a paper of Ward of 1961 dealing with prime divisors of the sequence of Lucas numbers $L = (L_n)$.

Sierpiński [65] considered the partition of the set of odd primes into two classes, the class A of primes that divide a number of the form 2^n+1 and the class B of primes dividing a number of the form $2^{2n+1}-1$. He observed that all primes $\pm 3 \pmod 8$ belong to A. Indeed, 2 is a quadratic nonresidue modulo such a prime p. Hence, by Euler's criterion, p divides $2^{\frac{p-1}{2}}+1$. On the other hand, primes $p \equiv 7 \pmod 8$ all belong to B. The integer 2 is then a quadratic residue modulo p. Hence, $p \mid 2^{\frac{p-1}{2}}-1$. But $(p-1)/2$ is odd. Thus, $p \in B$. In the remaining class, i.e., primes $1 \pmod 8$, it was noted that infinitely many were in A and that some belonged to B. All Fermat numbers $2^{2^m}+1$, $m \geq 2$, are pairwise coprime. Thus, if $p \mid 2^{2^m}+1$, then 2^{m+1} must be the order of 2 modulo p. Since $2^{m+1} \mid p-1$ for $m \geq 2$, we see that $p \equiv 1 \pmod 8$. Hence, as all Fermat numbers are coprime to one another, there are infinitely many primes dividing the sequence of Fermat numbers $(2^{2^m}+1)_{m\geq 2}$, and they must all lie in A. Brauer [22] noted that for $a \geq 2$ an integer, separating primes according to whether they divide a number a^n+1, or a number $a^{2n+1}-1$, comes down to partitioning according to the parity of the order of a modulo p. Thus, for $a=2$, A is the set of primes with respect to which the order of 2 is even, B for which it is odd. He also pointed out that for primes $1 \pmod 8$, if $2^e \,||\, p-1$, then $p \in B$ if and only if 2 is a 2^e-th power residue of p. Thus, the idea of splitting primes according to the exact power of 2 in $p-1$, which is essential to Hasse's method, began to emerge. Brauer also showed that infinitely primes $1 \pmod 8$ are in B. Indeed, for all primes $9 \pmod{16}$ representable by the quadratic form $65x^2+256xy+256y^2$, 2 is an octavic residue. He used the knowledge that if one prime of a given linear form is representable by a positive properly primitive quadratic form, then infinitely many primes of that linear form are representable by the quadratic form. Here, $73 \equiv 9 \pmod{16}$ and, for $x=3$, $y=-1$, $73=65x^2+256xy+256y^2$. In terms of prime density, these findings only gave that the lower density of A is at least $1/2$, and its upper density at most $3/4$. Possibly, the two sets A and B could still each be of density $1/2$. Hasse's method [30], presented in the next section, will show A to have a natural density of $17/24$, closer to $3/4$ than to $1/2$.

Given a second-order integral linear recurring sequence and an integer m, Ward [79] posed the important arithmetical question of deciding whether m is a divisor of the sequence. He argued that the problem can be reduced to finding out the prime divisors of the sequence. Thus, he dedicated his paper to a detailed investigation of the prime divisors of a particular sequence, the sequence $L=(L_n)$ of Lucas numbers – he calls them Fibonacci numbers of the second kind which explains the title of the paper.[†] By (2.8), we have:

$$L_n^2 - 5F_n^2 = 4(-1)^n. \tag{9.8}$$

[†] See our footnote on the appearance of the terminology "Lucas numbers" for the numbers of the sequence L, Chap. 1, p. 2.

Ward draws some interesting observations from (9.8). If a prime $p \equiv 1 \pmod 4$ divides L, then 5 must be a quadratic residue of p. By quadratic reciprocity, $p \equiv \pm 1 \pmod 5$. By contraposition, primes $1 \pmod 4$ and $\pm 2 \pmod 5$ do not divide L. Now suppose $p \equiv -1 \pmod 4$. Put $n = \rho$, the rank of p in the Fibonacci sequence, in (9.8). Then $L_\rho^2 \equiv 4(-1)^\rho \pmod p$. Since -1 is a quadratic nonresidue of p, ρ must be even. By Theorem 19, p is a prime divisor of (L_n). Alternatively, this result can be seen using Lemma 16, since $(-1 \,|\, p) = -1 \iff p \mid L_{(p-1)/2}$.

This information is summarized in a visual manner in Table 9.3.

Table 9.3 Elementary consequences of Equation (9.8)

	$p \equiv 1 \pmod 4$	$p \equiv -1 \pmod 4$
$p \equiv \pm 1 \pmod 5$	?	$p \mid L$
$p \equiv \pm 2 \pmod 5$	$p \nmid L$	$p \mid L$

Consequently, the lower and upper asymptotic densities of the set $\mathcal{P}(L)$ satisfy

$$\frac{1}{2} \le \underline{d}(L) \le \bar{d}(L) \le \frac{3}{4}.$$

It remained to study primes of the forms $20n+1$ and $20n+9$, for which both -1 and 5 are quadratic residues. For these primes, we have $k := \nu_2(p-1) \ge 2$. Setting $g_k(x) = x^{2^{k-1}} - x^{2^{k-2}} - 1$, Ward proves [79, Thm. 3.2] that $p \nmid L$ if and only if $g_k(x)$ splits completely into linear factors modulo p and $g_k(x^2)$ has no linear factors. This criterion is equivalent to how the Hasse-Lagarias method proceeds in order to find out the density of non-divisors of L. Had Ward been inclined to think in terms of density, he surely could have done so. Instead he found out criteria to determine whether primes of the forms $20n + 1$ or $20n + 9$ divide L. Such primes have a unique representation by the quadratic form $u^2 + 4v^2$, and, as easily checked, 5 must divide uv. Thus, Ward proves, for instance, that

$$p \mid L \iff u \text{ or } v \equiv \pm 1 \pmod 5.$$

We point out the existence of an efficient algorithm of Hermite, as improved by Brillhart [23], to find u and v. By Ward's criterion, we readily see that $101 = 1^2 + 4 \cdot 5^2$ divides L, whereas $109 = 3^2 + 4 \cdot 5^2$ does not. Similarly, $401 \mid L$, but $409 \nmid L$. More generally, all primes of the forms $1 + (5x)^2$ and $4 + (5x)^2$ divide L, while all primes of form $9 + (5x)^2$ do not.

The antecedents of the Hasse-Lagarias method are detectable both in Brauer's and Ward's papers.

9.5 The Hasse-Lagarias Method

Companion Lucas sequences $V = V(P, Q)$ are among the rare arithmetic sequences which, in the nondegenerate case, have been proven to possess a nontrivial natural density of prime divisors, i.e., a density $d = d(V)$ belonging to the open interval $(0, 1)$. Moreover, this density is a rational number, and, in principle, is computable. For instance, $d(V(4, 3)) = 2/3$, $d(V(3, 2)) = 17/24$ and $d(L) = 2/3$. The first two sequences are $(3^n + 1)$ and $(2^n + 1)$. In 1966, Hasse [30] developed a finely crafted method to evaluate the prime density of sequences $(a^n + 1)$, for a not $\pm$ a square. In particular, it fully answered the Sierpiński question. With the Hasse method, it is relatively easy to classify all densities of companion sequences $(a^n + b^n)$, when a and b are integers; see [80], [5, Thm. 3.1.3]. In 1985, Lagarias [35] showed the Hasse method could be extended to computing the prime density of certain second-order linear recurrences with irrational roots that include companion Lucas sequences.[†] In particular, he illustrated the method with the calculation of the prime density of the sequence L of Lucas numbers, thereby completing, at least in some sense, the work of Ward [79]. This explains the title of this section: The Hasse-Lagarias Method.

There is something nearly magical in associating with an arithmetic sequence, as simple as a second-order integral recurrence, a number in $(0, 1)$ which measures the size of its set of prime factors. People, mathematically versed or not, have often reacted with some curiosity at being told that on average, 17 out of 24 primes divide a number of the form $2^n + 1$. We have already seen that although defined as additive objects, Lucas sequences possess remarkable multiplicative features.

Even though density results are asymptotic by nature, experiments with prime divisors of linear recurrent sequences frequently show the proportion of divisors from a small collection of primes lining up closely with the asymptotic density value. This can provide a way of checking the calculated density as well as sometimes a chance at guessing its value, if the density is a simple rational number.

We provide a couple of tables, Tables 9.4 and 9.5, which illustrate this phenomenon. The first row gives the number n of primes tested for division. (We always tested the least primes $p_1, \ldots, p_n$.) The corresponding count of primes dividing V is indicated as c_V. The last row gives the number of primes expected to divide if the asymptotic proportion were to hold for the finite set $\{p_1, \ldots, p_n\}$.

[†] Lagarias rediscovered the method as he was initially unaware of the work of Hasse until Jean-Pierre Serre informed him of it (private communication).

Table 9.4 Prime divisors of $(3^x + 1)$ and of the sequence (L_x) of the Lucas numbers

n	30	60	90	120	150	180	210	240	270	300	...	900
$c_{(3^x+1)}$	20	39	59	78	98	121	139	157	176	198	...	601
c_L	19	39	58	82	99	121	141	163	185	206	...	599
'Expected'	20	40	60	80	100	120	140	160	180	200	...	600

Table 9.5 Prime divisors of $(2^x + 1)$

n	24	48	72	96	120	144	168	192	216	240	...	960
$c_{(2^x+1)}$	15	32	49	65	84	103	117	135	153	167	...	682
'Expected'	17	34	51	68	85	102	119	136	153	170	...	680

We now prove the Hasse density result for $d(V)$ when $V_n = a^n + 1$ and a is a square-free integer such that $|a| > 1$. The set of odd primes is the disjoint union of all $\mathcal{P}^j$, $j \geq 1$, where $\mathcal{P}^j = \{p : \ p \equiv 1 + 2^j \pmod{2^{j+1}}\}$. By the Dirichlet density theorem (9.4), $d(\mathcal{P}^j) = 1/\varphi(2^{j+1}) = 2^{-j}$. Observe that the densities $d(\mathcal{P}^j)$ sum up to 1. The Hasse method evaluates within each $\mathcal{P}^j$ the proportion of primes that divide no term of V. Put $N_j = \{p \in \mathcal{P}_j : \ p \nmid V\}$ and $D_j = \{p \in \mathcal{P}_j : \ p \mid V\}$. Suppose $p \nmid a$ and $p \in \mathcal{P}^j$. Let ρ be the order of $a \pmod p$. The number ρ is also the rank of appearance of p in $U(a+1, a)$. As seen in Theorem 19, $p \nmid V$ if and only if ρ is odd. Thus, $p \nmid V$ iff $a^{(p-1)/2^j} \equiv 1 \pmod p$, since 2^j is the full power of 2 in $p - 1$. Therefore, because $\mathbb{F}_p^*$ is cyclic, a is a 2^j-th power in $\mathbb{Z}/p\mathbb{Z}$. Hence, the polynomial $x^{2^j} - a$ has a root in $\mathbb{Z}/p\mathbb{Z}$. In fact, this polynomial factorizes completely modulo p since $\mathbb{Z}/p\mathbb{Z}$ contains 2^j-th roots of unity. By Remark 42, $p \equiv 1 \pmod{2^j}$ implies that p splits completely in $\mathbb{Q}(\zeta_{2^j})$. By the Kummer-Dedekind theorem, any prime ideal above p in $\mathbb{Q}(\zeta_{2^j})$ must split completely from $\mathbb{Q}(\zeta_{2^j})$ to $\mathbb{Q}(\zeta_{2^j}, \sqrt[2^j]{a})$. Therefore, p splits completely in the field $F_j := \mathbb{Q}(\zeta_{2^j}, \sqrt[2^j]{a})$. It does not split completely in $K_j := F_j(\zeta_{2^{j+1}})$ because $p \not\equiv 1 \pmod{2^{j+1}}$. By the Kronecker-Frobenius density theorem, N_j has density:

$$d(N_j) = \frac{1}{[F_j : \mathbb{Q}]} - \frac{1}{[K_j : \mathbb{Q}]}. \tag{9.9}$$

Suppose a is not ± 2. Then, $\sqrt{a}$ is not in $\mathbb{Q}(\zeta_{2^j})$. (The only quadratic number fields lying in $\mathbb{Q}(\zeta_8)$ are $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(\sqrt{-2})$.) Therefore, the degree of F_j over $\mathbb{Q}$ is

$$[\mathbb{Q}(\zeta_{2^j}) : \mathbb{Q}] \cdot [F_j : \mathbb{Q}(\zeta_{2^j})] = 2^{j-1} \cdot 2^j = 4^j/2. \tag{9.10}$$

Moreover, $[K_j : F_j] = 2$. Hence, $d(N_j) = 2 \cdot 4^{-j} - 4^{-j} = 4^{-j}$. The density of primes not dividing V is

$$\sum_{j \geq 1} d(N_j) = \frac{1}{4} \cdot \frac{1}{1 - 1/4} = \frac{1}{3}.$$

Thus, the complementary set, the set of prime divisors of V, has density $2/3$. To be rigorous, we should only have concluded that the lower asymptotic density of non-divisors, $\underline{d}(N)$, is at least $\lim_n \sum_{j=1}^{n} d(N_j) = 1/3$ since N contains $\cup_{j=1}^{n} N_j$ for all $n \geq 1$. But each D_j, being the complementary set of N_j in $\mathcal{P}_j$, has density $2^{-j} - 4^{-j}$. Since D contains $\cup_{j=1}^{n} D_j$ for all $n \geq 1$, $\underline{d}(D) \geq \lim_n \sum_{j=1}^{n} d(D_j) = 2/3$. Therefore, N, the complementary set of D in $\mathcal{P}$, has upper asymptotic density $\bar{d}(N)$ bounded above by $1/3$. The conclusion follows.

Suppose $a = \pm 2$. Then, $\zeta_8 = (\sqrt{a} + i\sqrt{a})/2$. Therefore, $F_2 = \mathbb{Q}(i, \sqrt[4]{a})$ contains ζ_8. As a result, $F_2 = K_2$ and, by (9.9), $d(N_2) = 0$. Also, the degrees of F_j and K_j, for $j \geq 3$, have been halved since $\mathbb{Q}(\zeta_j)$ now contains $\sqrt{a}$. Therefore,

$$\sum_{j \geq 1} d(N_j) = \frac{1}{4} + 0 + \sum_{j \geq 3} d(N_j) = \frac{1}{4} + \frac{1}{2} \sum_{j \geq 3} \frac{1}{4^{j-1}} = \frac{1}{4} + \frac{1}{24} = \frac{7}{24},$$

and the density of prime divisors of $(a^n + 1)$ is

$$d(2^n + 1) = d((-2)^n + 1) = 1 - \frac{7}{24} = \frac{17}{24}, \tag{9.11}$$

$(1/24)$-th more than $2/3$.

When the zeros α and β of $x^2 - Px + Q$ are quadratic irrationals, the same method applies, but the density computation is done in two separate steps. On the one hand, one computes the density of primes that split in $\mathbb{Q}(\alpha)$ and do not divide V; on the other, the density of primes inert in $\mathbb{Q}(\alpha)$ not dividing V. For the latter subset of primes, we fix $j \geq 1$ such $2^j \,||\, p + 1$ (rather than $p - 1$; for inert primes the rank of p divides $p + 1$) and evaluate for each such j the density of primes not dividing V much in the way done for $p - 1$. See [35] and [13, Chap. 6].

Lagarias enunciated sufficient conditions for an integral irreducible second-order linear recurring sequence $X = (a\alpha^n + \bar{a}\bar{\alpha}^n)_n$ to fall under the Hasse method: if there exists $\gamma \in \mathbb{Q}(\alpha)$ such that

$$\frac{\alpha}{\bar{\alpha}} = \pm\gamma^k \quad \text{and} \quad \frac{\bar{a}}{a} = \zeta\gamma^j, \tag{9.12}$$

where ζ is a root of unity in the field $\mathbb{Q}(\alpha)$, $k = 1$ or 2, and j is an integer, then one should be able to calculate unconditionally the prime density of $X = (a\alpha^n + \bar{a}\bar{\alpha}^n)_n$ by the Hasse-Lagarias method. (Here, $\bar{a}$ and $\bar{\alpha}$ denote the algebraic conjugates of, respectively, a and α within $\mathbb{Q}(\alpha)$.)

Companion Lucas sequences satisfy the Lagarias conditions (9.12); take $\gamma = \alpha/\bar{\alpha} = \alpha^2/Q$, $k = 1$, $j = 0$ and $\zeta = 1$. But there are integral second-order recurrences which are not companion Lucas sequences and satisfy (9.12). In fact, Lagarias [35] worked out the density for such a sequence. However, we

will observe in Sect. 9.7 that any recurrence satisfying (9.12) must be a torsion sequence in the Laxton group associated with the characteristic polynomial of the recurrence.

As mentioned earlier, the densities of companion Lucas sequences were fully described in [5, Thm. 3.1.3] in the case of reducible characteristic polynomials. No such description exists for all cases of irrational roots. However, Moree [42] gave the prime density for all companion Lucas sequences $V(P,-1)$. In these cases, $V_n = \epsilon^n + \bar{\epsilon}^n$, where $\epsilon = (P+\sqrt{P^2+4})/2$ is the fundamental unit in $\mathbb{Q}(\sqrt{P^2+4})$. But Moree and Stevenhagen [44] went further and worked out the densities of companion Lucas sequences $(\epsilon^n + \bar{\epsilon}^n)$, for all fundamental units ϵ of real quadratic fields $\mathbb{Q}(\sqrt{d})$, $(d > 1)$. If the norm of ϵ is -1 and $d > 2$, then the density is $2/3$. If the norm of ϵ is 1, the density is $1/3$, unless $(\epsilon + \bar{\epsilon})/2 + 1$ is a rational square. In 2007, Ljujić [39] wrote a Master's thesis under Stevenhagen's direction, where, in particular, $d(V)$ is shown to always be a rational number in $(0,1)$, and the values of $d(V)$ are given under various conditions on the irrational root α. Ballot [12] gave a proof that for almost all pairs of parameters (P,Q), $d(V(P,Q))$ is equal to $2/3$ in the sense that the set of exceptional pairs (P,Q), $|P| \le x$ and $|Q| \le x$, has cardinality $o(x^2)$ as $x \to +\infty$.

When the zeros α and β of $x^2 - Px + Q$ are rational integers, finding out the density of prime divisors of companion Lucas sequences boils down to discovering the density of primes p for which the order of a fixed rational number r modulo p is even. Considerable progress [52, Theorem 1.3], [43] has been made in the larger question of finding out uniform asymptotic estimates in m and x, where m is a positive integer, for the proportion of primes $p \le x$ for which the order of r modulo p is divisible by m. We will refer to this type of question as the *order divisibility problem*, or simply as the *order problem*. Hasse [31] had already considered the case when r is a rational integer and m is a prime number. Wiertelak [80], in the late 1970s, found some asymptotic estimates for the order problem when m is an exact prime power. To give an idea of the type of more advanced knowledge we have, here is a proposition [15, Lemma 2] based on results in Pappalardi's 2003 paper [52].

Proposition 137 Suppose $a > 1$ is an integer, but not an integer's k-th power for any $k \ge 2$, and m is an odd positive integer. Let $\ell_a(p)$ be the order of a modulo p, where $p \nmid a$ is a prime number. Define $A = \{p \ ; \ m \mid \ell_a(p)\}$. Then, for all $\epsilon > 0$, the estimate

$$\#A(x) = \left(d_m + O\left(\frac{m^{1-2\epsilon}}{(\log x)^{\frac{1}{8}-\epsilon}}\right)\right)\pi(x),$$

holds uniformly in m and x with

$$d_m = \frac{1}{m}\prod_{q \mid m}\frac{q^2}{q^2-1}, \quad (q \text{ prime}).$$

As the concept of the rank of a prime in a fundamental Lucas sequence U generalizes the order of a rational number, finding out the proportion of primes for which $m \mid \rho_U(p)$, m a positive integer, is a natural generalization of the order problem. The successful study of the case when $x^2 - Px + Q$ has irrational zeros came years later. Several 1998 conjectures in the Fibonacci case $U = F$, made on experimental grounds by Bruckman and Anderson [24], concerning the frequency with which $\rho_F(p)$ is divisible by a given positive integer m, or is divisible by an exact power of a prime, were proved in 2014 by Cubre and Rouse [25]. The first conjecture stipulated that the set of primes p for which $m \mid \rho_F(p)$ has the density:

$$d_m = \frac{c_m}{m} \cdot \prod_{q \mid m} \frac{q^2}{q^2 - 1}, \quad (q \text{ prime}), \tag{9.13}$$

where c_m is a correction factor equal to $5/4$, if $m \equiv 10 \pmod{20}$, $1/2$, if $20 \mid m$, and 1, otherwise. Thus, for instance, primes with a Fibonacci rank divisible by 30 have density:

$$d_{30} = \frac{5}{4} \cdot \frac{1}{30} \cdot \frac{2 \cdot 2}{3} \cdot \frac{3 \cdot 3}{8} \cdot \frac{5 \cdot 5}{24} = \frac{5}{4} \cdot \frac{2}{3} \cdot \frac{3}{8} \cdot \frac{5}{24} = \frac{1}{16} \cdot \frac{25}{24}.$$

An important contribution to the nondegenerate irreducible case was made by Sanna [59] in 2020; he obtained an asymptotic formula for $\#A(x)$ in the form $d_m \pi(x)$, plus an error term which depends on U and m. Here, m is an *odd* positive integer (not divisible by 3 in case $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-3})$) and A is the set of primes p for which $m \mid \rho_U(p)$. Then,

$$d_m = \frac{c_m}{m} \cdot \prod_{q \mid m} \frac{q^2}{q^2 - 1}, \quad (q \text{ prime}), \tag{9.14}$$

where

$$c_m = \gcd(m^\infty, h)^{-1} + \eta_U(m),$$

h is the largest exponent such that $\alpha/\beta = \gamma^h$, for some $\gamma \in \mathbb{Q}(\alpha)$, and $\eta_U(m)$ is 0, most of the time, i.e., if $D > 0$, or $D_0 \not\equiv 1 \pmod 4$, or $D_0 \nmid m^\infty$, but depends explicitly on $\gcd(m^\infty, h)$ and the square-free part D_0 of $D = P^2 - 4Q$, otherwise. Here, m^∞ is the formal product $\prod_{p \mid m} p^\infty$. Thus, if x is an integer, then $\gcd(x, m^\infty)$ is the product of all prime powers p^ν, where $p \mid \gcd(x, m)$ and $p^\nu \,||\, x$.

The particular cases when $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-3})$ and $m = 3$ or 6 were dealt with in another context [13, Theorem 6.9]. The "usual" densities in these instances are $d_3 = 3/4$ and $d_6 = 1/2$. The densities d_2 and d_4 when $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-1})$, Q not the square of an integer, nor twice such a square, are $d_2 = 5/6$ and $d_4 = 2/3$ [13, Theorem 6.2].

Remark 44 Before closing this section, we point out that much work has been done on prime divisors of the general integral second-order linear recurrence. In 1921, Pólya showed [54] the linear recurrence $(c_1a^n+c_2b^n)_n$ has an infinite number of prime divisors, if a, b, c_1, c_2 are nonzero integers, and $r_1^x r_2^y \neq 1$ for all x and y in $\mathbb{Z}$, unless $x = y = 0$, where $r_1 = a/b$ and $r_2 = -c_2/c_1$. In 1954, Ward [77] showed any integral second-order nondegenerate linear recurrence has infinitely many prime divisors. Some of these sequences are so-called "torsion" sequences – see Sect. 9.7.1, and companion Lucas sequences are among them. But for the general non-torsion second-order recurrence, following Hooley's idea on Artin's conjecture, density results, conditional on the truth of generalized Riemann hypotheses, were obtained by Stephens [67] in 1976, and, in 2000, were refined and corrected by Moree and Stevenhagen [45]. For the general non-torsion second-order linear recurrence $X = (c_1a^n + c_2b^n)_n$, a, b integers, the prime density of X, is expressed in the form

$$d(X) = C_X \cdot \prod_{p \text{ prime}} \left(1 - \frac{p}{p^3 - 1}\right) := C_X \cdot S, \tag{9.15}$$

where the above product S, over all primes p, was introduced by Stephens and C_X is a positive corrective constant that depends on X, which often lies in a small interval around 1 (see [45, p. 303]). The value of the Stephens constant S is approximately 0.57596. Moree and Stevenhagen [46] challenged themselves, with success, to find, under Riemann hypotheses, the prime density of the second-order linear recurrence Y, mentioned by Lagarias [35, p. 451], with $Y_0 = 3$ and $Y_1 = 1$, which satisfies the same recursion as the sequence L of Lucas numbers, i.e., $Y_{n+2} = Y_{n+1} + Y_n$, $(n \geq 0)$. Note that Y has irrational roots, but their result is again expressed in the form $\delta(Y) = C_Y \cdot S$, where $C_Y = \frac{1\,573\,727}{1\,569\,610} \simeq 1.0026$, and S is the Stephens constant.

9.6 A Heuristic View

Why is it that primes that divide even-indexed terms V_{2n} are so often twice as many as primes dividing odd-indexed terms V_{2n+1}? Even though we have the Hasse-Lagarias method and a precise argument to say that for most choices of pairs (P, Q) this phenomenon holds, one cannot but feel that simple intuition is eluding us on why it should be true. Shouldn't they split equally between the two categories? We recall John Selfridge at the WCNTC,[†] probably in the late 1990s, with his distinctive red sweater, saying during one of his interventions, with a grin on his face, that he had an idea why this held. Quizzing him later on his remark didn't bring an "ah, hah" moment. The

[†] The West Coast Number Theory Conference; it was held at Asilomar, a conference center near Monterey, California, as we recall in that instance.

question lingered and we felt this was a later heuristic view, somewhat in the way Daniel Shanks (see [62, 63] and [64, pp. 80–83]) used to proceed, which brought about a satisfactory intuitive answer.

A first simple version of these heuristics was presented in [9, Sect. 5]. If a is a positive integer and d_a is the density of primes p for which the order of $a \pmod p$ is odd, then, using, say Theorem 3.1.3 in [5], it is a simple matter to prove that $\lim_N N^{-1} \sum_{1\le a\le N} d_a = 1/3$. Perhaps as a nod to Wang-Wei's quotation that started the chapter, we may reverse the point of view. Fixing a prime p, the heuristic argument evaluates the proportion of positive integers a whose order modulo p is odd, to find again an expected mean of $1/3$. These heuristics were pursued and used in Sects. 2 and 3 of [12] for general and specific sets of primes p defined by $2 \nmid \rho_U(p)$. In particular, the case $U = F$ was treated. They were later applied [13, Sect. 6.3] to the cases $m \nmid \rho_U(p)$ when **1.** $D = -E^2$, $m = 2$ and 4, and **2.** $D = -3F^2$, $m = 2$, 3 and 6, where E and F are integers.

Let us look at the simplest case: prime divisors of $(a^n + 1)$, where $a \in \mathbb{Z} \setminus \mathbb{Z}^2$, $a \neq -1$, $a \neq \pm 2$. We may ignore the finitely many primes that divide $2a$. Hence, we assume $a \in \mathbb{Z}_p^*$. The heuristic follows the Hasse method. We evaluate the density of primes p for which the order h_p of $a \pmod p$ is odd. Partition the primes into the sets $\mathcal{P}^j = \{p : \ p \equiv 1 + 2^j \pmod{2^{j+1}}\}$, for $j \ge 1$. The heuristic part of the argument consists of assigning a probability P_j for a random prime p in $\mathcal{P}^j$ not to divide $(a^n + 1)$. If $p \in \mathcal{P}^j$, then the number of 2^j-th power residues in $\mathbb{Z}_p^*$ is $(p-1)/2^j$, i.e., the order of the group $\langle g^{2^j} \rangle$, generated by g^{2^j}, where g is a primitive root modulo p. Assuming $a \pmod p$ to be a random element in $\mathbb{Z}_p^*$ as p varies in $\mathcal{P}^j$, its chances of hitting a 2^j-th power residue are $2^{-j}(p-1)/(p-1)$, that is, 2^{-j}. Note that h_p is odd if and only if $a \pmod p$ is a 2^j-th power residue modulo p. Hence, we put $P_j = 2^{-j}$. Since the weight of $\mathcal{P}^j$ in the set of all primes is given by its density, which, by the Dirichlet theorem, is 2^{-j}, the heuristic predicts that

$$d(a^n + 1) = 1 - \sum_{j\ge 1} d(\mathcal{P}^j) \cdot P_j = 1 - \sum_{j\ge 1} 4^{-j} = 1 - \frac{1}{3} = \frac{2}{3},$$

which is the density proved by Hasse. The heuristics [12, p. 135] for $a = \pm 2$ have to be modified because for $j = 2$, $p \equiv 5 \pmod 8$ and a is necessarily a quadratic nonresidue of p, whereas if $j \ge 3$, then $p \equiv 1 \pmod 8$, and a, on the contrary, is necessarily a quadratic residue of p.

Let us try to work out these heuristics for the set of primes p whose Fibonacci rank $\rho_F(p)$ is a multiple of 10. By (9.13), these primes have density $\frac{1}{6} \cdot \frac{25}{24}$. Here, $F = U(1,-1)$, α and β are the zeros of $x^2 - x - 1$, $D = 5$ and $V = L$, the sequence of Lucas numbers. Suppose $p \equiv \pm 2 \pmod 5$. By Theorem 9, $\rho \mid p + 1$. But $5 \nmid p + 1$. Hence, $5 \nmid \rho$. Similarly, if $p \equiv -1 \pmod 5$, then $10 \nmid \rho(p)$. Indeed, $\rho \mid p-1$, but $5 \nmid p-1$. It remains to examine primes $1 \pmod 5$. Suppose $p \equiv 3 \pmod 4$. By Lemma 15, $p \mid L_{(p-1)/2}$.

Thus, by Theorem 19, $2 \mid \rho$. Therefore, $10 \mid \rho$ if and only if $5 \mid \rho$. Let $\mathcal{P}_5^j = \{p\,;\ 5^j \,||\, p-1\}$, $j \geq 1$. By the Dirichlet density theorem, $\mathcal{P}_5^j$ has density $4/\varphi(5^{j+1}) = 5^{-j}$. Assume further that $p \in \mathcal{P}_5^j$. Then, $5 \nmid \rho$ iff $(\alpha/\beta)^{(p-1)/5^j} \equiv 1 \pmod{p}$, which occurs iff α/β is a 5^j-th power modulo p. The proportion of 5^j-th power residues modulo p in $\mathbb{Z}_p^*$ is 5^{-j}. Assuming $-\alpha^2 = \alpha/\beta \pmod{p}$ is as likely as any other member of $\mathbb{Z}_p^*$ to hit a 5^j-th power residue as p varies in $\mathcal{P}_5^j$, we expect a density of

$$\sum_{j\geq 1} d\big(\mathcal{P}_5^j \cap \{p\,;\ p \equiv 3 \pmod 4\}\big) \cdot 5^{-j} = \frac{1}{2}\sum_{j\geq 1} 25^{-j} = \frac{1}{48}, \tag{9.16}$$

of primes $p \equiv 11 \pmod{20}$ such that $5 \nmid \rho(p)$. It follows that primes $11 \pmod{20}$ with $5 \mid \rho$ have density:

$$\frac{1}{8} - \frac{1}{48} = \frac{5}{48}. \tag{9.17}$$

Consider now primes $1 \pmod 4$, that is, primes $1 \pmod{20}$. Thus, we are dealing with a set of primes of density $1/8$. Suppose $2^j \,||\, p-1$ for some $j \geq 2$. Then, $\rho(p)$ is odd iff $(-\alpha^2)^{(p-1)/2^j} \equiv 1 \pmod{p}$. This occurs iff $-\alpha^2$ is a 2^j-th power residue modulo p. The number of 2^j-th power residues in $\mathbb{Z}_p^*$ is $(p-1)/2^j$. However, since -1 is a square modulo p, $-\alpha^2$ is a quadratic residue modulo p. The odds of $-\alpha^2$ hitting a 2^j-th power residue are then $2^{-j}(p-1)/2^{-1}(p-1) = 2^{1-j}$. Primes $p \equiv 1 \pmod 5$ with $2^j || p-1$ have density $4^{-1} \cdot 2^{-j}$. Therefore, we expect primes $1 \pmod{20}$ with odd rank to have density:

$$\sum_{j\geq 2} 2^{-(2+j)} \cdot 2^{1-j} = \frac{1}{2}\sum_{j\geq 2} 4^{-j} = \frac{1}{24}.$$

This is saying that the probability of primes $1 \pmod{20}$ to have odd rank is $1/3$. Thus, their probability of having even rank is $2/3$. Assuming the independence of the two events "p has even rank" and "p has rank divisible by 5," we find that $10 \mid \rho$ with probability

$$\frac{2}{3} \cdot \text{prob}\big(5 \mid \rho,\ \text{if } p \equiv 1 \pmod{20}\big) = \frac{2}{3} \cdot \frac{5}{6} = \frac{5}{9}.$$

The 5/6-th probability above comes from carrying out the very same calculations that led to the densities in (9.16) and (9.17), only replacing primes $3 \pmod 4$ in (9.16) by primes $1 \pmod 4$. Thus, the density of primes with rank divisible by 5 among primes $1 \pmod{20}$ is $5/48$. This yields the claimed probability of $(5/48)/(1/8) = 5/6$. Since primes $1 \pmod{20}$ have density $1/8$, our heuristics give the density:

$$\frac{5}{9} \cdot \frac{1}{8} = \frac{5}{72},$$

for primes $1 \pmod{20}$ and rank divisible by 10. Summing 5/72 and 5/48, we get a density of

$$\frac{5}{24}\left(\frac{1}{3}+\frac{1}{2}\right)=\frac{25}{6\cdot 24},$$

the correct density! Some readers will surely enjoy finding similar heuristics for $m = 20$.

As seen in the above, these heuristics only use the Dirichlet density theorem, the cyclic structure of $\mathbb{Z}_p^*$, and some simple equidistribution assumptions. In Sect. 9.8, we will see that comparable heuristics apply to finding the density of sets of primes that divide higher-order linear recurrences, but where division is defined in ways other than the usual one.

Remark 45 If $U(P, Q)$ is a regular Lucas sequence, then, extending the result of Matiyasevich and Guy [41] for the Fibonacci sequence, Kiss and Mátyás [33] proved that

$$\lim_{n\to\infty}\frac{\log|[U_1,U_2,\ldots,U_n]|}{\log|\prod_{k=1}^{n}U_k|}=\frac{6}{\pi^2}, \tag{9.18}$$

where $[*, *, \ldots, *]$ stands for the least common multiple. We may view (9.18) as another manifestation of the strong divisibility property of a regular $U(P, Q)$. From [20], the above ratios, with the terms $U_k(P, Q)$ replaced by $V_k(P, Q)$, have a limit equal to $\frac{8}{\pi^2}$. Perhaps, this result is to be put in relation with the common prime density $d(V) = 2/3$. Note that, if instead of terms of Lucas sequences U or V, one puts [17] sequences of type $\alpha^n - \zeta_m\beta^n$, where ζ_m is a primitive m-th root of unity, with $m = 3$ or 6 if $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-3})$, and $m = 4$, if $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-1})$, one also obtains limits for the corresponding ratios, namely, $135/(16\pi^2)$, $234/(25\pi^2)$, and $80/(9\pi^2)$, when m is 3, 6, and 4, respectively.

9.7 The Laxton Group and Its Generalizations

9.7.1 The Laxton Group

In 1969 and 1970, Robert Laxton published two rich papers [37, 38] that dealt with integral second-order linear recurrences and their prime divisors. He constructed a semigroup structure $F(f)$ on the set of linear recurrences that share a common characteristic polynomial f of degree two. The product in this semigroup has the property that it preserves division by primes. That is, if p is a prime, $p \mid X$ and $p \mid Y$, then $p \mid X * Y$, where $X * Y$ represents the semigroup product of the two sequences X and Y. By "identifying" two sequences if they differ merely by an index shift, or if they are rational scalar multiples of one another, then one gets a set of equivalence classes, $G(f)$, on which the semigroup operation in $F(f)$ is well defined and makes $G(f)$ a

group. Moreover, division by primes is still preserved by the group operation. A prime p divides a class in $G(f)$ if there is a sequence X in that class such that $p \mid X_n$, but $p \nmid X_{n+1}$, for some index n. This division of X is called *proper division*. Suppose $X \in F(f)$. If $p \mid X$, then either p is a proper divisor of X or it is a *null divisor*, i.e., p divides all terms from some point onward. The distinction between the usual division and proper division is minimal as Ward [76, 77] showed an X in $F(f)$ possesses at most a finite number of null prime divisors. The fundamental Lucas sequence $U(P,Q)$ and its companion $V(P,Q)$ have a central place in the group $G(f)$. Indeed, $U(P,Q)$ is the identity element of $F(f)$ and the class of $V(P,Q)$ has order 2 in $G(f)$, and this class is, for most $f(x)$, the only nontrivial torsion element in $G(f)$. Many subgroups and quotient subgroups were studied and identified in [37]. The last pages of [37] and the second paper [38] are devoted to properties of torsion elements, and a complete description of $T(f)$, the torsion subgroup of $G(f)$.

Besides Laxton's papers, partial descriptions of the Laxton group or references to its structure have appeared in various places in the literature [5, pp. 15–18], [26, Sect. 1.1.7]. More recently, several mathematicians from Japan have worked on finding group theoretical descriptions for the structure of the Laxton group [2, 3, 69–71]. Nevertheless, we briefly present, in the Laxton manner, this group here again.

Given $f(x) = x^2 - Px + Q \in \mathbb{Z}[x]$, $PQ \neq 0$, $P^2 \neq 4Q$, Laxton defined the set $F(f)$ of nongeometric linear recurring sequences (X_n), which have integer terms from some point onward and satisfy:

$$X_{n+2} = PX_{n+1} - QX_n.$$

If α and β are the zeros of $f(x)$, then there are nonzero algebraic integers A and B such that

$$X_n = \frac{A\alpha^n - B\beta^n}{\alpha - \beta}, \tag{9.19}$$

for all integers n. We find that $A = x_1 - x_0\beta$, $B = x_1 - x_0\alpha$ and write the sequence X as $\langle A, B\rangle$. The semigroup operation $*$ in $F(f)$ is defined by

$$X * X' = \langle AA', BB'\rangle, \tag{9.20}$$

if $X = \langle A, B\rangle$ and $X' = \langle A', B'\rangle$. As easily verified, the initial values y_0 and y_1 of the product sequence $Y := X * X'$ satisfy

$$\begin{cases} y_0 = x_0x_1' + x_0'x_1 - Px_0x_0', \\ y_1 = x_1x_1' - Qx_0x_0', \end{cases} \tag{9.21}$$

where x_0, x_1 and x_0', x_1' are the respective initial terms of X and X'. Thus, $AA' = y_1 - y_0\beta$ and $BB' = y_1 - y_0\alpha$. One readily sees from (9.21) that if $p \mid x_0$ and $p \mid x_0'$, then $p \mid y_0$. (In fact, if in addition $p \nmid x_1$ and $p \nmid x_1'$,

then $p \nmid y_1$. Thus, proper division is preserved in $F(f)$, and, thus, division of classes in $G(f)$ is also preserved.)

Two sequences X and Y in $F(f)$ are defined to be equivalent, and we write $X \sim Y$, if and only if there is an integer s and a rational number r such that

$$x_n = r y_{n+s},$$

for all indices n. The semigroup operation $*$ is well defined on equivalence classes of sequences. Moreover, $G(f)$, the set of classes, together with the operation $\bar{*}$ derived from $*$, forms an abelian group. The inverse of the class of $\langle A, B\rangle$ is the class of $\langle B, A\rangle$. One may observe that $\langle B, A\rangle$ belongs to $F(f)$ since B is

$$x_1 - x_0\alpha = x_1 - x_0(P-\beta) = (x_1 - Px_0) - (-x_0)\beta, \text{ (or } (-Qx_{-1}) - (-x_0)\beta).$$

By (9.19), we have $U = \langle 1, 1\rangle$, and, by (9.20), the class of the fundamental Lucas sequence U is seen to play the role of the identity element of the group $G(f)$. Also, $V = \langle P - 2\beta, P - 2\alpha\rangle = \langle \alpha - \beta, \beta - \alpha\rangle$. Hence,

$$V * V = \langle D, D\rangle = D\langle 1, 1\rangle = D \cdot U,$$

and we see that the class of V is a torsion element of order 2 in $G(f)$.

In [35], Lagarias computed the prime density of three second-order linear recurrences: $(2^n + 1)$, (L_n) and a certain sequence (W_n). Their respective prime densities were 17/24 (as first shown by Hasse), 2/3 for the Lucas numbers as mentioned in Sect. 9.5 and 3/4 for (W_n). The first two are companion Lucas sequences; the third one is not. However, (W_n) has order three in the Laxton group associated with $f(x) = x^2 - 5x + 7$. This is readily checked: $W_0 = 1$ and $W_1 = 2$; the zeros of $f(x)$ are $(5 \pm \sqrt{-3})/2$. Thus, if $W = \langle A, B\rangle$, then $A = 2 - \beta$, where $\beta = (5 - \sqrt{-3})/2$. Therefore,

$$A = 2 - \frac{5 - \sqrt{-3}}{2} = \frac{-1 + \sqrt{-3}}{2} = \zeta_3,$$

the third root of unity $e^{2i\pi/3}$. Hence,

$$W * W * W = \langle A^3, B^3\rangle = \langle \zeta_3^3, (\bar{\zeta}_3)^3\rangle = \langle 1, 1\rangle = U(5, 7).$$

In fact, to date, all second-order linear recurrences for which the prime density is unconditionally known all belong to the torsion subgroup $T(f)$ of some $G(f)$.[†] The group $G(f)$ is infinite, while $T(f)$ is finite. In fact, $T(f)$ often consists solely of the classes of the fundamental and the companion Lucas sequences $U(P, Q)$ and $V(P, Q)$.

[†] However, with the use of generalized Riemann hypotheses, one can find the prime density of other second-order recurrences – see [45, 46], or Remark 44 of this book.

We saw earlier that Lagarias gave sufficient conditions (9.12) for a second-order linear recurrence to fall under the Hasse-Lagarias method. It was shown [5, pp. 20–22] that the class of a sequence obeying the Lagarias conditions must be of finite order in $G(f)$; in fact, its order must divide 12. Given $f = (x - \alpha)(x - \bar{\alpha})$, the set $L(f)$ of classes of recurrences which satisfy the Lagarias conditions (9.12) forms a subgroup of the torsion group $T(f)$. (There are polynomials $f(x)$ for which $L(f)$ is a proper subgroup of $T(f)$; see [5, Prop. 2.4.5].)

When the root field $\mathbb{Q}(\alpha)$ contains cube roots of unity, and hence sixth roots of unity and $D = (\alpha - \bar{\alpha})^2 \in -3\mathbb{Z}^2$, $T(f)$ contains at least a cyclic subgroup of order six. Similarly, if $\mathbb{Q}(\alpha)$ contains fourth roots of unity and $(\alpha - \bar{\alpha})^2 \in -\mathbb{Z}^2$, then $T(f)$ contains a cyclic subgroup of order four. Williams' paper [82] – unrelated to Laxton's point of view – develops properties of the sequences of order three or six when $\mathbb{Q}(\alpha)$ contains $e^{2i\pi/3}$, in particular, properties leading to primality tests à la Lucas for numbers of certain types. Ballot's long paper [13] studies the six "torsion" sequences when $D = -3F^2$, and the four 'torsion' sequences when $D = -E^2$, F and E integers, from many points of view. The purpose was to bring convincing evidence that these second-order integral linear recurrences ought to be viewed as purebred Lucas sequences (i.e., authentic companion Lucas sequences only of orders 3, 6, and 4 instead of 2 for (V_n)). That is, for discriminants of the form $D = -E^2$, there are four Lucasian sequences G, H, V, and U, where $G_0 = H_0 = 1$, $G_1 = (P + E)/2$, $H_1 = (P - E)/2$; for D of the shape $-3F^2$, there are six: Y, Z, S, T, V, and U. The (W_n)-sequence, of which Lagarias computed the 3/4-th prime density, is an S, or a T, sequence (depending on the sign given to F, since $S_0 = T_0 = 1$ and S_1 and T_1 are $(P \pm F)/2$). We have $Y_0 = Z_0 = 1$ and Y_1, Z_1 are $(P \pm 3F)/2$. For instance, most of the important formulas given in Chap. 2 involving U and V have analogues involving G and H, or S, T, Y, and Z. Many arithmetic properties have their counterparts too. To give only a few examples, the double-angle formula (2.23), i.e., $U_{2n} = U_n V_n$, has the counterparts [13, Eqs. (2.28), (2.61)]:

$$\begin{aligned} U_{4n} &= 2U_n V_n G_n H_n, && \text{if } D = -E^2; \\ U_{6n} &= 3U_n V_n S_n T_n Y_n Z_n, && \text{if } D = -3F^2. \end{aligned}$$

The Euler criterion for Lucas sequences (Theorem 36) has analogues that decide when a prime p divides $X_{(p-\epsilon_p)/4}$, for $X = U, V, G$ or H, if $D = -E^2$, or when $p \mid X_{(p-\epsilon_p)/3}$, $X = U, S$ or T, if $D = -3F^2$. We saw in Theorem 19 that prime divisors of the V sequence are those with an even rank ρ_U. When $D = -E^2$, the G and the H sequences share the same prime divisors by Laxton's semigroup law: the class of one is the cube of the class of the other, and the group law preserves prime division. Except for primes dividing $2Q$, prime divisors of G, or H, are the primes with a rank ρ_U divisible by 4.

Likewise, when $D = -3F^2$, primes with a rank ρ_U divisible by 3 are the divisors of the S and the T sequences; those with a rank divisible by 6 are the divisors of the Y and the Z sequences, which are of order 6 in the Laxton group. As mentioned in Sect. 5.8, the fact that the sum $\sum_{0<t<\rho} \frac{V_t}{U_t}$ is zero modulo p^2 when ρ is maximal has analogues involving the pairs (G, H), (S, Z), and (T, Y), all of which differ by a factor of V with respect to the Laxton group law. For instance, say f has discriminant $D = -E^2$. Then, we have $V * G = E \cdot H \sim H$, where $*$ is the semigroup operation in $F(f)$. If $p \nmid QE$ is a prime of maximal rank $\rho = \rho_U = p - \epsilon_p$, then $\sum_{\rho_H<t<\rho_H+\rho} \frac{G_t}{H_t}$ is zero modulo p^2, where ρ_H is the least positive h such that $p \mid H_h$. Since $\epsilon_p = (-E^2 \,|\, p)$, the rank ρ_H exists because $4 \mid p - \epsilon_p$. We saw in Sect. 9.5 that in some precise sense, for almost all choices of parameters (P, Q), the prime density of $V(P, Q)$ is 2/3. Results in the same vein have been shown for the V and G sequences which, for almost all discriminants of the form $-E^2$, have respective prime densities 5/6 and 2/3. Similarly, the V, S, and Z sequences have respective prime densities 2/3, 3/4, and 1/2, for almost all discriminants of the from $-3F^2$; see [13, Chap. 6].

Given $f(x) = x^2 - Px + Q$ in $\mathbb{Z}[x]$, Laxton [37, Thm. 4.4] proves that $T(f)$ contains three elements of order *two* if and only if $Q = R^2$, where $R \in \mathbb{Z}$. The two other elements besides the class of $V(P, Q)$ come from the sequences $A = (A_n)_{n\geq 0}$ and $B = (B_n)_{n\geq 0}$ with respective initial values 1 and $P \pm R$. The four classes of U, V, A, and B thus form a copy of the Klein group. Laxton observes [37, Thm. 4.6] that

$$U_{2n+1} = A_n \cdot B_n,$$

and that the sets of prime divisors of A and B are disjoint. It follows that the sets of prime divisors of the three order-two sequences A, B, and V form a *three*-block partition of the set of all primes,[†] the primes of odd rank dividing either A or B, those of even rank dividing V.

There are cases when each of the three blocks of the partition have equal prime density, i.e., a density of 1/3. For instance, if $\epsilon = a + b\sqrt{d}$ is a fundamental unit of norm -1 in the ring of integers of a real quadratic field $\mathbb{Q}(\sqrt{d})$, ($d \geq 3$ squarefree), then the A, B and V torsion sequences associated with $x^2 - (4a^2 + 2)x + 1 = (x - \epsilon^2)(x - \bar{\epsilon}^2)$ has each prime density 1/3; see [14]. Up to a constant, we find that $A_n = V_{2n+1}(P, -1)$, $B_n = U_{2n+1}(P, -1)$ and $V_n(P^2 + 2, 1) = V_{2n}(P, -1)$, where $P = 2a$. Let ρ be the rank of primes with respect to $U(P, -1)$. Then, primes dividing B have odd rank ρ, primes dividing A satisfy $2 \,||\, \rho$, and primes dividing $V(P^2 + 2, 1)$ have a rank ρ with 2-adic valuation greater than or equal to 2. For $\epsilon = (1 + \sqrt{5})/2$, Vinson [74]

[†] but possibly the prime factors of Q

observed that if T_F is the period of the Fibonacci sequence modulo a prime p, and $\rho_F(p)$ its rank in the Fibonacci sequence, then $T_F = m_F(p) \cdot \rho_F$, where the multiplier $m_F(p)$ may only take the values 1, 2, or 4. Prime divisors of the three order-two torsion sequences A, B, and V with respect to $x^2 - 3x + 1$ have the alternate respective characterizations $m_F(p) = 1$, $m_F(p) = 4$ and $m_F(p) = 2$, each set having density 1/3 [14]. In particular, the prime density of the Lucas numbers (L_n), which Lagarias [35] proved to be 2/3, is the set of primes satisfying $m_F(p) = 1$ or 2.

If Q is a square and $D = -3F^2$, then the group generated by the classes of A and one of the order-six sequences, say Y, is a subgroup of $T(f)$ isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_6$. If instead $D = -E^2$, then $T(f)$ contains a subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$.

Let us examine an example in more detail. For $f(x) = x^2 - 2x + 49$, we find that $D = -3 \cdot 8^2$. Thus, $F = 8$ and the group $\langle A, Y \rangle$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_6$. In Table 9.6, for each of the 12 sequences X, we counted the number of primes p, when p varies from $p_1 = 2$ to $p_{200} = 1223$, which divide at least one term among $X_2, X_3, \ldots, X_{p+1}$. Below, we indicate our (educated) guess for their prime density (something that can be checked using the Hasse-Lagarias method and the Laxton group properties to alleviate some of the work). Since Y and Z have respective initial values 1 and $(P \pm 3F)/2$, we computed the two initial values, using equations (9.21), for each sequence. We got $U = [0, 1]$, $Y = [1, 13]$, $S = [1, 5]$ $(\sim Y^2)$, $V = [2, 2]$ $(\sim Y^3)$, $T = [1, -3]$ $(\sim Y^4)$, $Z = [1, -11]$ $(\sim Y^5)$, $A = [1, -5]$, $A * Y = [6, -114] = 6 \cdot [1, -19]$, $A * S = [-2, -74] = -2 \cdot [1, 37]$, $A * V \sim B = [1, 9]$ (we used B instead of $A * V$), $A * T = [-10, -34] = -2 \cdot [5, 17]$ and $A * Z = [-18, 6] = 6 \cdot [-3, 1]$.

Table 9.6 Twelve torsion sequences and their prime divisors

Sequence	U	Y	S	V	T	Z
# Prime divisors	199	49	149	67	149	49
Conjectured prime density	1	1/4	3/4	1/3	3/4	1/4
Sequence	A	$A * Y$	$A * S$	$A * V$	$A * T$	$A * Z$
# Prime divisors	69	50	52	63	52	50
Conjectured prime density	1/3	1/4	1/4	1/3	1/4	1/4

Using a probabilistic terminology, we may guess from the data that the two events "$2 \mid \rho$" and "$3 \mid \rho$" are independent. Indeed, one-third of the primes divide V. Three-fourths of the primes divide S, i.e., have a rank divisible by 3. Now $2 \mid \rho$ and $3 \mid \rho \iff 6 \mid \rho$, and we note that the product $1/3 \times 3/4$ yields the "probability" 1/4, which is the prime density of Y, i.e., of primes whose rank is divisible by 6.

9.7.2 Generalizations of the Laxton Group

There is a generalization of the Laxton group, discovered in [5], which is well-suited to prime maximal division.[†]

Suppose $X = (X_n)_{n\geq 0}$ is an integral linear recurrence with monic characteristic polynomial $f(x)$ in $\mathbb{Z}[x]$ of degree $m \geq 2$. Let p be a prime number. Then, p is a (prime) *maximal divisor* of X if and only if there are exactly $m-1$ consecutive terms of X divisible by p, i.e., if and only if

$$p \mid X_i,\ i = n,\ n+1, \ldots, n+m-2,\ \text{but } p \nmid X_{n+m-1}, \tag{9.22}$$

for some index n.

The concept was introduced by Ward [78] in 1954 and generalizes the notion of proper divisor for $m = 2$ mentioned in the previous subsection.

The fundamental recurrence U with $U_0 = U_1 = \ldots = U_{m-2} = 0$ and $U_{m-1} = 1$, which is an extension of the fundamental Lucas sequence to all $m \geq 2$, obviously has every prime as a maximal divisor; in fact, it is known [60, 66] that all recurrences in $F(f)$ with a density of prime maximal divisors equal to 1 are in the class of U. The generalized Laxton group for maximal division will have the class of U for its identity element. Classes are defined as previously, i.e., two sequences in $F(f)$ belong to the same class if some index shift and multiplication by a rational number applied to one sequence yields the second sequence. As noted by Ward [78, Eq. (2.4)], all integral linear recurrences X with characteristic polynomial f, assuming f has m distinct zeros $\alpha_1, \alpha_2, \ldots, \alpha_m$, have the form:

$$X_n = \sum_{i=1}^{m} A_i \frac{\alpha_i^n}{f'(\alpha_i)}, \tag{9.23}$$

where f' is the derivative of f and the A_i's are algebraic integer constants in the root field of f. The set $F(f)$ is limited to the integral linear recurrences of exact order m, i.e., satisfying $\prod_{i=1}^{m} A_i \neq 0$.

Representing the sequence X in (9.23) as $\langle A_1, A_2, \ldots, A_m\rangle$ and assuming $Y = \langle B_1, B_2, \ldots, B_m\rangle$, we define the operation $*$ on $F(f)$ by

$$X * Y = \langle A_1B_1, A_2B_2, \ldots, A_mB_m\rangle.$$

The product sequence $X * Y$ is an integral linear recurrence, and $(F(f), *)$ is an abelian semigroup with identity. The identity is the fundamental recurrence U which turns out to be $\langle 1, 1, \ldots, 1\rangle$ [5, pp. 76–77]. The sequence

[†] In 1994, one of the authors, C. Ballot, was invited to Cambridge, UK, by R. Pinch to give a couple of lectures on the material developed in [5]. The stay was memorable in several ways, including the experience of some of the traditions unique to the place. R. Laxton had taken the train from Nottingham to attend the first lecture. He was overjoyed that some then-young mathematician had at last done something with his early discoveries.

$$\langle B_1, \ldots, B_j, \ldots, B_m \rangle,$$

where $B_j = \prod_{1 \le i \le m;\ i \ne j} A_i$, $(1 \le j \le m)$, belongs to $F(f)$, and its class is the inverse of the class of $X = \langle A_1, \ldots, A_j, \ldots, A_m \rangle$ in $(G(f), \bar{*})$, where $\bar{*}$ is the well-defined operation: Class of X $\bar{*}$ Class of Y = Class of $(X * Y)$.

It was shown in [5, §5 Chap. 5] that when $f(x)$ has m nonzero rational roots, then $G(f)$ contains a subgroup $M(f)$ isomorphic to $\mathbb{Z}_2^{m-1}$. Hence, there are $2^{m-1} - 1$ distinct class recurrences which are torsion of order *two*. (If $m = 2$, then $M(f)$ is simply the group with two elements generated by the class of the companion Lucas sequence.)

A notion of *rank*, ρ, or $\rho_{\max}$, of maximal division for a prime p is now introduced. It is, if it exists, the least positive index n such that

$$p \mid U_i,\ i = n, n+1, \ldots, n+m-2,\ \text{but } p \nmid U_{n+m-1}, \tag{9.24}$$

where U is the fundamental recurrence. By definition, maximal division of X occurs *at* n iff

$$p \mid X_n,\ p \mid X_{n+1}, \ldots,\ p \mid X_{n+m-2},\ \text{but } p \nmid X_{n+m-1}. \tag{9.25}$$

Maximal division of $X = \langle A_1, \ldots, A_m \rangle$ occurs at n iff

$$A_1 \alpha_1^n \equiv A_2 \alpha_2^n \equiv \cdots \equiv A_m \alpha_m^n \pmod{(p)}, \tag{9.26}$$

where (p) is the ideal generated by p in the ring of integers of the root field of f, and the congruence holds in that ring.

It is not difficult to see that $p \mid_{max} U$ at n if and only if $\rho \mid n$. Thus, given an integer $s \ge 2$ finding out the prime density, assuming existence, of

$$\{p;\ s \mid \rho_{\max}(p)\} \tag{9.27}$$

is a reasonable extension of the order problem mentioned in Sect. 9.5.

Particular attention was given to the cubic case in Chap. 4 of [5]. In that case a maximal divisor divides two consecutive terms of the sequence. Given an abelian group $(G, *)$ and an element a in G, one can easily construct an isomorphic group $(G, +)$ with identity element a. It suffices to define the operation $+$ by $x + y = x * y * a^{-1}$, for all x and y in G, where a^{-1} is the inverse of a in $(G, *)$. Using this remark, it was shown that we may favor other kinds of division than maximal division. For instance, we may favor the notion of *twin division*. Say p is a twin divisor of X if and only if there is some $n \ge 1$ such that

$$p \mid X_{n-1},\ p \mid X_{n+1},\ \text{but } p \nmid X_n.$$

It was proved that the aforementioned isomorphism from the generalized Laxton group $(G(f), *)$ to $(G(f), +)$ using $a = T$, where T is the recurrence with cubic characteristic polynomial $f(x)$ and initial values $[0, 1, 0]$, has the

additional property that it transforms maximal divisors of a given element into twin divisors of its image. Thus, in particular, any density computation of the set of maximal divisors of a given recurrence (or equivalently of its class) corresponds to the density of twin divisors of its image through the isomorphism.

The above generalization of the Laxton group, we recall, was done assuming the m zeros of $f(x)$ to be distinct. Another relevant group [6] was discovered in the case $f(x)$ has exactly one double zero. The nth Cullen number, C_n, is defined as $C_n = n2^n + 1$. Robinson [56] showed all Cullen numbers C_n, $2 \le n \le 1000$, were composite, except for C_{141}. Here is, in our context, a striking property of the Cullen numbers, not unrelated to their high level of compositeness. Suppose p is an odd prime. Then, by Fermat's theorem, we see that

$$\begin{aligned} C_{p-2} &= (p-2)2^{p-2} + 1 \equiv -2^{p-1} + 1 \equiv 0 \pmod{p}, \\ C_{p-1} &= (p-1)2^{p-1} + 1 \equiv -1 + 1 \equiv 0 \pmod{p}, \\ C_p &= p2^p + 1 \equiv 1 \pmod{p}. \end{aligned} \tag{9.28}$$

That is, every prime $p \ge 3$ is a maximal divisor of the third-order recurrence $(C_n)_{n\ge 0}$. Yet, it is not equivalent, in the Laxton sense, to the fundamental recurrence U with initial values $[0, 0, 1]$. Suppose $f(x) = (x-\alpha)^2(x-\beta) \in \mathbb{Z}[x]$ and write $f_1(x) = (x-\alpha)(x-\beta)$ for the squarefree part of f. Then, there is a generalized Cullen-number recurrence $(C_f(n))_{n\ge 0}$, namely,

$$C_f(n) = \left(\frac{n}{\alpha - \beta} - \frac{2\beta - \alpha}{(\alpha - \beta)^2} \right) \alpha^n + \frac{\beta}{(\alpha - \beta)^2} \beta^n, \tag{9.29}$$

in $F(f)$ which satisfies, for all primes $p \nmid \alpha\beta(\alpha - \beta)$,

$$C_f(p-2) \equiv C_f(p-1) \equiv 0 \quad \text{and} \quad C_f(p) \equiv 1 \pmod{p}. \tag{9.30}$$

It turns out that by broadening, or, as one may prefer to say, by weakening the notion of equivalence used by Laxton, we obtain a relevant group $G(f)$, in which the generalized Cullen-number recurrence and the fundamental recurrence belong to the same class. Incidentally, it remains true that only the identity class contains recurrences with a density of maximal prime divisors equal to one. Moreover, there is an isomorphism from $G(f)$ to the Laxton group $G(f_1)$ which sends all maximal prime divisors to proper divisors of the image. If $f(x) = (x-1)(x-2)^2$, then the class of the sequence $(n2^n - 1)_{n\ge 0}$ is sent onto the class of the companion Lucas sequence $(2^n + 1)_{n\ge 0}$, which was seen in Sect. 9.5 to possess a 17/24 density of prime divisors. Hence, 17 out of 24 primes on average divide two consecutive terms of $(n2^n - 1)$. We do not know whether relevant group structures exist whenever there are two double zeros, or one triple zero.

Recently Suwa [72] wrote a preprint reformulating in terms of affine group schemes the aforementioned isomorphism between $G(f)$ and $G(f_1)$.

9.8 The Density of Maximal Prime Divisors

It is possible to extend the Hasse-Lagarias method to compute the exact prime density of maximal divisors of some torsion recurrences of the generalized Laxton group $G(f)$, where $f \in \mathbb{Z}[x]$ is monic of degree $m \geq 3$. The Hasse-Lagarias method can also solve, in some cases, the generalized order problem as stipulated in (9.27). As mentioned in Sect. 9.7, if the roots of f are nonzero distinct integers, then the torsion subgroup $T(f)$ of $G(f)$ contains a subgroup $M(f)$ isomorphic to $\mathbb{Z}^{m-1}$. The generic maximal prime density of a recurrence whose class belongs to an order-two element of $M(f)$ is $2/(2^m-1)$ (see [5, Prop. 5.5.5]). Note that for $m = 2$, we recover the common 2/3-density of a companion Lucas sequence.

If $f(x) = (x-\alpha)(x-\beta)(x-\gamma) = x^3 - Px^2 + Qx - R$, where α, β and γ are three distinct nonzero integers, then the three order-two recurrence classes in $M(f)$ have for representants $V_1 = [2, 2\alpha, P\alpha - \beta\gamma]$, $V_2 = [2, 2\beta, P\beta - \alpha\gamma]$, and $V_3 = [2, 2\gamma, P\gamma - \alpha\beta]$. They can be written respectively as $\langle -A, A, A\rangle$, $\langle B, -B, B\rangle$, and $\langle C, C, -C\rangle$, for some nonzero integers A, B, and C. Using (9.23), we easily see that p is a maximal divisor of V_1 iff for some $n \geq 1$:

$$\left(\frac{\alpha}{\beta}\right)^n \equiv \left(\frac{\alpha}{\gamma}\right)^n \equiv -1 \pmod{p},$$

which can be translated into the equivalent condition

$$\nu_2(h_1) = \nu_2(h_2) \geq 1,$$

where h_1 and h_2 are the orders of α/β and α/γ modulo p. The above conditions permit one to start a Hasse-Lagarias process. If $\alpha_i \neq \pm r^2\alpha_j$ or $\alpha_i \neq \pm 2r^2\alpha_j$, where α_i, α_j are two of the zeros α, β, or γ, and r is a rational number, then each V_i, $i = 1, 2$ or 3, has a density of maximal divisors equal to 2/7; see [5, Prop. 4.6.4]. The three sets of maximal prime divisors of the V_i's, $1 \leq i \leq 3$, are disjoint. Hence, their union has density 6/7 under the above conditions on the zeros of f. This union is also $\{p;\ 2 \mid \rho_{\max}(p)\}$ providing an answer to a case of the generalized order problem (9.27). One may refer to [5, Thm. 5.6.5] for some answer to the generalized order problem, when $s = q$, a prime, and f has degree $m \geq 2$ and m distinct zeros in $\mathbb{Z}$.

Thus, the density of primes dividing two consecutive terms of $(5^n + 2\cdot 3^n - 1)$ is $2/7 \simeq 0.286$; it is $65/224 \simeq 0.290$ for the recurrence $(3^n - 2^{n+1} - 1)$, where one zero is twice another. This is to be compared with the fact that the prime density of $(2^n + 1)$, which is 17/24, is a notch higher than that of $(3^n + 1)$,

which is 2/3. In fact, 17/24 and 65/224 obey the same formula: $\frac{4^m+1}{4^m} \cdot \frac{2}{2^m-1}$, for $m = 2$ and 3, respectively.

These densities lend themselves well to the type of heuristics encountered in Sect. 9.6. We illustrate this with two examples.

Heuristics for Two Cubic Recurrences

1. Let $M_n = 5^n + 2 \cdot 3^n - 1$ for $n \geq 0$. We present a simple probabilistic argument that yields a prime density of 2/7 for the set

$$A = \{p\ ;\ p \nmid 30,\ p \mid \gcd(M_n, M_{n+1}) \text{ for some } n\}.$$

Let p be a prime in A. Then, p divides M_n and M_{n+1} if and only if

$$p \mid M_{n+1} - 3M_n \quad \text{and} \quad p \mid M_{n+1} - 5M_n.$$

But $M_{n+1} - 3M_n = 2 \cdot 5^n + 2$ and $M_{n+1} - 5M_n = -4 \cdot 3^n + 4$. Thus, $p \in A$ if and only if there is an $n \in \mathbb{N}$ for which the system (S_M) of exponential congruences

$$(S_M): \begin{cases} 5^n \equiv -1 \pmod{p}, \\ 3^n \equiv -1 \pmod{p}, \end{cases} \tag{9.31}$$

is solvable. Let h_1 and h_2 be the respective orders of 5 (mod p) and 3 (mod p). Then, (9.31) is solvable if and only if h_1 and h_2 are both even and n is an odd multiple of both $h_1/2$ and $h_2/2$. But these conditions hold exactly when we have

$$\nu_2(h_1) = \nu_2(h_2) \geq 1.$$

Thus, $A = \{p\ ;\ p \nmid 30,\ \nu_2(h_1) = \nu_2(h_2) \geq 1\}$. Let us fix $j \geq 1$ and evaluate the probability P_j that a prime p satisfying $\nu_2(p-1) = j$ be in A. For any k, $1 \leq k \leq j$, $\nu_2(h_1) = k$ if and only if 5 is a 2^{j-k}-th power residue, but not a 2^{j+1-k}-th power residue (mod p). The proportion of such power residues in $(\mathbb{Z}/p\mathbb{Z})^*$ being equal to

$$\left[(p-1)/2^{j-k} - (p-1)/2^{j+1-k}\right]/(p-1) = 2^{-j-1+k},$$

the probability that $\nu_2(h_1) = k$ is assumed to be 2^{-j-1+k}. The same assumptions are made if we replace 5 by 3. Therefore, we have:

$$\begin{aligned} P_j &= \sum_{k=1}^{j} \text{Prob}_{\nu_2(p-1)=j}\{\nu_2(h_1) = k\} \times \text{Prob}_{\nu_2(p-1)=j}\{\nu_2(h_2) = k\} \\ &= \sum_{k=1}^{j} (2^{-j-1+k})^2 = \sum_{l=1}^{j} 4^{-l} = \frac{1}{3}(1 - 4^{-j}). \end{aligned}$$

The density of primes d_j satisfying $\nu_2(p-1) = j$ being 2^{-j}, our expected density for A is obtained by summing over j

$$\sum_{j\geq 1} d_j \times P_j = \frac{1}{3}\left[\sum_{j\geq 1} 2^{-j} - \sum_{j\geq 1} 8^{-j}\right] = \frac{1}{3}\left[1 - \frac{1}{7}\right] = \frac{1}{3}\cdot\frac{6}{7} = \frac{2}{7}.$$

2. Let us consider the cubic recursion $T_n = 3^{n+1} + 2^{n+3} - 5,\ n \geq 0$. We now present a heuristic yielding the prime density of the set

$$B = \{p\ ;\ p \nmid 30,\ p \mid \gcd(T_n, T_{n+2}) \text{ for some } n\}.$$

Recall that if a prime p divides both the n-th term and $n+2$-th term of a cubic recursion (X_n) for some $n \geq 0$, then we say that p is a twin divisor of (X_n).

Since $T_{n+2} - 4T_n = 15\,(3^n + 1)$ and $T_{n+2} - 9T_n = 40\,(-2^n + 1)$, a prime p lies in B if and only if the system of exponential congruences

$$(S_T): \begin{cases} 3^n \equiv -1 \pmod{p}, \\ 2^n \equiv 1 \pmod{p}, \end{cases} \tag{9.32}$$

is solvable in n. Letting h_1 and h_2 be the respective orders of 2 and 3 $\pmod{p}$, (S_T) is solvable if there is some odd multiple n of $h_2/2$ which is also a multiple of h_1. This holds exactly when $\nu_2(h_2) \geq 1 + \nu_2(h_1)$. Fixing $j \geq 1$, let P_j denote the probability that $\nu_2(h_2) \geq 1 + \nu_2(h_1)$ as p varies through primes satisfying $\nu_2(p-1) = j$. Thus,

$$P_j = \sum_{k=0}^{j-1} \text{Prob}\{\nu_2(h_1) = k\} \times \text{Prob}\{\nu_2(h_2) \geq 1 + k\}.$$

Hence, $P_1 = \text{Prob}\{\nu_2(h_1) = 0\} \times \text{Prob}\{\nu_2(h_2) = 1\} = 1/2 \times 1/2$, since we expect 2 to be a quadratic residue of p for half the primes $p \equiv 3 \pmod{4}$, and we expect the same proportion holds true for 3. For $j = 2$, $p \equiv 5 \pmod{8}$ so 2 is a quadratic non-residue of p. Therefore, $\nu_2(h_1) = 2$ and $P_2 = 0$, since $\nu_2(h_2)$ cannot exceed 2. For $j \geq 3$, 2 is a quadratic residue of p. Now, for k, $0 \leq k \leq j-1$, $\nu_2(h_1) = k$ implies that 2 is a 2^{j-k}-th power, but not a 2^{j-k+1}-th power $\pmod{p}$. The proportion of 2^{j-k}-th power residues which are not 2^{j-k+1}-th power residues *among* quadratic residues is

$$\big((p-1)/2^{j-k} - (p-1)/2^{j+1-k}\big) \ /\ \big((p-1)/2\big) = 2^{-j+k},$$

for $1 \leq k \leq j-1$. And for $k = 0$ this same proportion is

$$\big((p-1)/2^{j}\big) \ /\ \big((p-1)/2\big) = 2^{-j+1},$$

since $\nu_2(p-1) = j$ implies that there are no 2^{j+1}-th power residues $\pmod{p}$.

Thus, we assume $\text{Prob}\{\nu_2(h_1) = k\}$ to be 2^{-j+1} if $k = 0$, and 2^{-j+k} if $1 \leq k \leq j-1$. A similar argument gives:

$$\text{Prob}\{\nu_2(h_2) \geq 1 + k\} = \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^{j-k}} = 1 - 2^{-j+k}.$$

Therefore, we evaluate P_j, $j \geq 3$, as

$$2^{-j+1} \times (1 - 2^{-j}) + \sum_{k=1}^{j-1} 2^{-(j-k)} \times (1 - 2^{-(j-k)}) = \frac{2}{3}(1 - 4^{-j}),$$

after summing and simplifying. The expected prime density of B is given by the sum

$$\begin{aligned} \sum_{j \geq 1} 2^{-j} \times P_j &= \frac{1}{8} + 0 + \sum_{j \geq 3} 2^{-j} \times \frac{2}{3} \times (1 - 4^{-j}) \\ &= \frac{1}{8} + \frac{2}{3} \cdot \frac{1}{4} - \frac{2}{3} \cdot \frac{1}{8^3} \cdot \frac{1}{1 - 1/8} \\ &= \frac{7}{24} - \frac{1}{24 \times 28} = \frac{195}{24 \times 28} = \frac{65}{224}. \end{aligned}$$

As mentioned earlier, there is a corresponding cubic linear recurrence in $F(f)$, where $f = (x-1)(x-2)(x-3)$, which has B as its set of maximal prime divisors.

Early experimental data suggested that when f is a cubic polynomial with three linear factors over $\mathbb{Z}[x]$, the general non-torsion cubic linear recurrences in $G(f)$ have very few maximal prime divisors; see the first two tables in [5, p. 44]. Partial results showing, indeed, this density to be 0 were achieved in [15, 16]. The two above heuristics – see Eqs. (9.31) and (9.32) – show a prime p is a maximal, or a twin divisor, of a cubic recurrence if and only if a system of two congruences of the shape

$$a^n \equiv b \pmod{p} \quad \text{and} \quad c^n \equiv d \pmod{p},$$

is solvable in n. In particular, in [16], the case where the rank of the group $\langle a, b, c, d \rangle$, generated by a, b, c, and d in $\mathbb{Q}^*$, is at most 2, is examined in detail.

If $f(x) = x^3 - Px^2 + Qx - R = (x - \alpha)(x - \bar{\alpha})(x - c)$, where α is a quadratic algebraic integer, $\bar{\alpha}$ is its algebraic conjugate and c is a nonzero integer, then only one of the three recurrences (V_i) in $M(f)$ has rational integer terms, namely, the recurrence with initial values $T = [2, 2c, Pc - \alpha\bar{\alpha}]$. The class of T has order 2 in the generalized Laxton group $G(f)$. If $c = 1$ and α is a fundamental unit of norm -1 of a quadratic field $\mathbb{Q}(\sqrt{d})$, $d \geq 3$, then $T_n = 1 + U_{n-1} + U_n$, where U is the Lucas sequence $U(\alpha + \bar{\alpha}, -1)$. If $\alpha = (1 + \sqrt{5})/2$, then $T_n = 1 + F_{n+1}$ and its density of maximal divisors, i.e., of primes p for which two consecutive Fibonacci numbers are congruent to -1 modulo p, was computed in [7]; it is equal to $2/3$. (It is the set of primes for which the multiplier $m_F(p)$ is either 2 or 4 – see the end of Sect. 9.7.1.)

As explained in Sect. 6.4, if D is a non-cube integer and $\delta = \sqrt[3]{D}$, raising a fundamental solution $\alpha = X_1 + Y_1\delta + Z_1\delta^2$ of the cubic Pell equation

$$x^3 + Dy^3 + D^2z^3 - 3Dxyz = 1, \tag{9.33}$$

to the n-th power, $n \in \mathbb{Z}$, yields all integer solutions of equation (9.33). The algebraic conjugates of α are $\beta = X_1 + Y_1\omega^2\delta + Z_1\omega\delta^2$ and $\bar{\beta}$, the complex conjugate of β, where $\omega = e^{2i\pi/3}$. Put $f(x) = (x-\alpha)(x-\beta)(x-\bar{\beta}) \in \mathbb{Z}[x]$. Define (X_n), (Y_n) and (Z_n) by

$$X_n + \delta Y_n + \delta^2 Z_n = \alpha^n,$$

for all n. Then, we find that

$$\begin{aligned} 3X_n &= \alpha^n + \beta^n + \bar{\beta}^n, \\ 3\delta Y_n &= \alpha^n + \omega\beta^n + \omega^2\bar{\beta}^n, \\ 3\delta^2 Z_n &= \alpha^n + \omega^2\beta^n + \omega\bar{\beta}^n, \end{aligned}$$

i.e., we get, up to a factor of 3, a set of Williams' sequences. These sequences were the object of the doctoral thesis [81] and were discussed in Sect. 6.5.

Remarkably, it was shown in [8], given $M > 1$, $\epsilon = \pm 1$, $D = M^3 + \epsilon \neq 0$, where it is known that $\alpha = M^2 + M\delta + \delta^2$ is a fundamental solution to (9.33), that writing the recurrences $(3X_{n-1})$, $(3Y_{n-1})$ and $(3Z_{n-1})$ in their standard form (9.23) yields:

$$\langle \delta^2, \delta^2\omega, \delta^2\omega^2 \rangle, \quad \langle \delta, \delta\omega^2, \delta\omega \rangle \quad \text{and} \quad \langle 1, 1, 1 \rangle.$$

This readily shows that the class of X is a torsion element of order *three* in the generalized Laxton group $G(f)$. This class generates a group of order *three* containing the class of Y, also of order *three*, and the class of Z, the identity element.

The density of maximal divisors of X, or of Y, is generically equal to $51/104$, i.e., a tiny bit less than $1/2$.[†] The ranks $\rho_{\max}$ of all prime maximal divisors of X, or Y, are multiples of 3, but there are primes not dividing X or Y such that $3 \mid \rho_{\max}$. In fact, it was shown that the set $\{p;\ 3 \mid \rho_{\max}(p)\}$ generically has the density $157/312$, i.e., slightly more than $1/2$. This is the case, for instance, when $M = 7$ and $\alpha = 4 + 2\sqrt[3]{7} + \sqrt[3]{49}$. The method of proof is again an extension of the Hasse-Lagarias method, with the caveat that for companion Lucas sequences $(V(P,Q)(n) = \alpha^n + \beta^n)$, where $P^2 - 4Q$ is not a perfect square, the Hasse-Lagarias method required computing separately the density of prime divisors according to whether they split, or remained inert in $\mathbb{Q}(\sqrt{P^2 - 4Q})$. Here, the method computes separately three cases: primes 2 (mod 3), which split into three prime ideals in $\mathbb{Q}(\delta, \omega)$; primes 1 (mod 3) such that D is not a cube modulo p which split into two prime ideals; and

[†] As noted by H. Roskam (private communication) and, later, P. Moree (Mathscinet Review of [8]), there are exceptions, not pointed out in [8], where the density differs from the generic value quoted herein.

primes 1 (mod 3) for which D is a cube modulo p which split into six prime ideals in $\mathbb{Q}(\delta, \omega)$.

There may be other irreducible cubic polynomials:

$$f(x) = x^3 - Px^2 + Qx - R = (x - \alpha)(x - \beta)(x - \gamma) \in \mathbb{Z}[x]$$

such that $G(f)$ contains torsion elements for which the density of maximal divisors may be calculated through a similar method, and perhaps, other f's for which $(\alpha^n + \beta^n + \gamma^n)$ is also torsion of order *three*. Much remains to be discovered.

9.9 Irreducible Polynomials Dividing $(X^n + 1)_n$ in $\mathbb{F}_q[X]$

Lucas sequences are sequences of rational integers, but many of the identities they satisfy would hold in other rings than the ring $\mathbb{Z}$. Indeed, if $\mathcal{R}$ is a ring (with 1) and P and Q are nonzero elements of $\mathcal{R}$, then one may define the pair of Lucas sequences $U(P, Q)$ and $V(P, Q)$, as we did in Chap. 2, by their initial conditions $U_0 = 0$, $U_1 = 1$; $V_0 = 2$, $V_1 = P$, and the common recursion:

$$X_{n+2} = PX_{n+1} - QX_n,$$

for all $n \geq 0$.

Their arithmetic properties could offer some variations worthy of curiosity, or of interest. If p is a prime and $e \geq 1$ an integer, then we denote the field with $q = p^e$ elements by $\mathbb{F}_q$. A few arithmetic properties of Lucas sequences in the ring $\mathbb{F}_q$ were studied in [48]. To our knowledge, no detailed study of the arithmetic of Lucas sequences in the ring $\mathbb{F}_q[X]$, of polynomials over $\mathbb{F}_q$, has been undertaken.

However, the rings $\mathbb{Z}$ and $\mathbb{F}_q[X]$ share much in common. Both are euclidean rings. The $q - 1$ elements of $\mathbb{F}_q^*$ replace the two invertibles ± 1 of $\mathbb{Z}$. Monic polynomials correspond to the positive integers $\mathbb{N}$. Monic irreducible polynomials in $\mathbb{F}_q[X]$ correspond to prime numbers in $\mathbb{N}$. Thus, we will often use the term *primes* in $\mathbb{F}_q[X]$ for monic irreducible polynomials. The number of primes in $\mathbb{F}_q[X]$ of degree n, $(n \geq 1)$, is denoted by I_n. It satisfies the well-known formula:

$$I_n = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d},$$

where μ is the Möbius function introduced in Sect. 4.3, and the sum is over all positive divisors d of n. It is an easy matter to verify than $I_n \sim q^n/n$, as $n \to \infty$. This asymptotic equivalence between I_n and q^n/n is usually referred to as the prime number theorem (PNT) for the ring $\mathbb{F}_q[X]$. Indeed, q^n is the number of monic polynomials of degree n in $\mathbb{F}_q[X]$, and $n = \log_q(q^n)$. Thus, the quotient q^n/n is an analogue of the classical PNT, $\pi(x) \sim x/\log x$. The

norm $|P|$ of a monic polynomial P of degree $n \geq 1$ is the cardinality of the quotient ring $\mathbb{F}_q[X]/P$, i.e., $|P| = q^n$. Thus, there is a definition of Dirichlet, or analytic density analogous to (9.2). If S is a set of primes in $\mathbb{F}_q[X]$, then S is said to have analytic density $\delta = \delta(S) \in [0, 1]$ if and only if the limit

$$\lim_{s \to 1^+} \frac{\sum_{P \in S} |P|^{-s}}{\sum_P |P|^{-s}} \tag{9.34}$$

exists and is equal to δ. There are, in the $\mathbb{F}_q[X]$ context, analogues of the Dirichlet, the Kronecker-Frobenius, and the Cebotarev density theorems which ensure sets of primes possess an analytic density as defined in (9.34). The notion of natural density which seems to be used most often is the following. If $S \subset I$, where I is the set of primes in $\mathbb{F}_q[X]$, and the limit

$$\lim_{n \to \infty} \frac{S_n}{I_n} \tag{9.35}$$

exists, then it is the density of S. Here, S_n is the number of primes in S of degree n. In [9], the density (9.35) is referred to as the d_1-density of S. Perhaps, one compelling reason why d_1 is often considered a sensible analogue of the usual natural density of rational primes is that $d_1(S)$ exists if and only $d_2(S)$ exists, where $d_2(S)$, provided it exists, is defined as

$$\lim_{N \to \infty} \left(\sum_{n=1}^{N} S_n \right) / \left(\sum_{n=1}^{N} I_n \right).^{\dagger} \tag{9.36}$$

The d_2-density is cumulative, whereas d_1 is local to degree n primes. But because of the fast growth of I_n with n, the two densities d_1 and d_2 are equivalent in the Murata sense – see the end of Sect. 9.1; refer to [9, Prop. 1.8] for a proof of the equivalence between d_1 and d_2. According to Bilharz, a hint that the d_2-density is not an appropriate analogue of the classical natural prime density, came from Davenport. Bilharz proves [21] that the set of primes P in $\mathbb{F}_p[X]$ having X as a primitive root, i.e., such that the order of X in the multiplicative group of the finite field $\mathbb{F}_p[X]/(P)$, is $p^n - 1$, where P has degree n, does not have a d_2-density. In the classical setting, primes having a given integer a as primitive root are, under Riemann hypotheses, known to possess a natural density [32]. Thus, Bilharz's result came as a surprise.

Consider the companion Lucas sequence $V(X + 1, X) = (V_n)$ in $\mathbb{F}_q[X]$ with initial values 2 and $X + 1$ and defining recursion:

$$V_{n+2} = (X + 1) \cdot V_{n+1} - X \cdot V_n, \quad (n \geq 0).$$

---

† Another reason is that the PNT in $\mathbb{F}_q[X]$ only considers primes of degree n. See also [57, Thm. 9.13B] for a version of the Cebotarev density theorem valid with respect to d_1-density.

It turns out [10] that the Hasse method is valid in this context, and the analytic densities of prime divisors of the sequence of polynomials $V_n = X^n+1$ can be computed for all prime powers q. For instance, if $q = 3$, we find that

$$\delta(\{P \text{ prime};\ P \mid V_n,\ \text{for some } n\}) = 17/24, \tag{9.37}$$

where $P \mid V_n$ means that there is a $\Lambda \in \mathbb{F}_q[X]$ such that $P \cdot \Lambda = V_n$. But these sets won't generally have a d_2-density. In [9], a detailed discussion led to the conclusion that another notion of density, called d_3, was a better analogue of natural density than d_1, or d_2. A set $S \subset I$ possesses a d_3-density, $d_3(S)$, equal to

$$\lim_{N\to\infty} N^{-1} \sum_{n=1}^{N} \frac{S_n}{I_n}, \tag{9.38}$$

provided this limit exists. In fact, it is possible [10] through an elementary method, which does not use the versions of the Kronecker-Frobenius or Cebotarev theorems in $\mathbb{F}_q[X]$, to see directly that prime divisors of the V-sequences, such as (9.37), have a d_3-prime density. Hence, by (9.37), primes P such that the order of X modulo P in $\mathbb{F}_q[X]$ is odd have d_3-density 7/24. As in the classical case, a numeric check is feasible. Thus, $7/24 \simeq 0.2917$, and it was calculated [10, Rmk. 4.6] that $r_{11} \simeq 0.2868$, where $r_N = N^{-1} \sum_{n=1}^{N} S_n/I_n$ is the N-th approximant to the d_3-density. Note that since, in the Murata sense, we have [9]:

$$\delta \prec d_3 \prec d_2,$$

the elementary method implies the analytic densities of those sets. Primes P in $\mathbb{F}_q[X]$ for which X is a primitive root of P do not have a d_1-density, but they do have a d_3-density [9, pp. 322–324].

Suppose ℓ is an odd prime number. If a is an integer, not an ℓ-th power in $\mathbb{Z}$, then the classical Hasse method ([31], [5, Thm. 3.2.3]) yields the natural density $\ell/(\ell^2 - 1)$ for the set of rational primes:

$$\{p;\ \ell \text{ divides the order of } a \pmod p\}. \tag{9.39}$$

(For $\ell = 2$, we often have a 2/3-density which the same formula $\ell/(\ell^2 - 1)$ provides correctly.)

The elementary method of [10] was extended further [11] to show the set of primes, analogous to (9.39), i.e.,

$$\{P \in \mathbb{F}_q[X];\ \ell \text{ divides the order of } X \pmod P\} \tag{9.40}$$

has a d_3-density equal to

$$\frac{1}{f}\left(1 - \frac{1}{\ell^{\nu-1}(\ell+1)}\right),$$

where ℓ is an odd prime, f is the order of $q \pmod{\ell}$ and $\nu = \nu_\ell(q^f - 1)$. We note that if q is a primitive root modulo ℓ and $\nu = 1$, then the above density yields, as in the classical case, $\ell/(\ell^2 - 1)$.

The papers [9–11] have barely opened the door to the problem of determining the prime density of companion Lucas sequences in $\mathbb{F}_q[X]$. For instance, one may ask whether it is possible to extend the elementary method that proved prime divisors of $V(X+1, X)$ have d_3-density to the companion sequence $V(X, -1)$? Note that the discriminant associated with $V(X+1, X)$ is $(X-1)^2$, but the discriminant of $V(X, -1)$, $D = X^2 + 4$, is not a square in $\mathbb{F}_q[x]$, if $q = p^e$, $p \geq 3$. (For $p = 2$, $D = (X+2)^2$.)

References

1. Şaban, Alaca and Kenneth S. Williams, *Introductory Algebraic Number Theory*, Cambridge University Press, 2004. xviii+428 pp.
2. M. Aoki and Y. Sakai, *mod p equivalence classes of linear recurrence sequences of degree 2*, Rocky Mountain J. Math. **47** (2017), no. 8, 2513–2533.
3. M. Aoki and M. Kida, *On the Laxton group*, Res. Number Theory **5** (2019), no. 1, Paper No. 13.
4. Tom M. Apostol, *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.
5. C. Ballot, *Density of prime divisors of linear recurrences*, Mem. Amer. Math. Soc., 551, (1995), 102 pp.
6. C. Ballot, *Group structure and maximal division for cubic recursions with a double root*, Pacific J. Math. **173** (1996), no. 2, 337–355.
7. C. Ballot, *The density of primes p, such that -1 is a residue modulo p of two consecutive Fibonacci numbers, is* 2/3, Rocky Mountain J. Math. **29** (1999), no. 3, 749–761.
8. C. Ballot, *Strong arithmetic properties of the integral solutions of $X^3 + DY^3 + D^2Z^3 - 3DXYZ = 1$, where $D = M^3 \pm 1$, $M \in \mathbb{Z}^*$*, Acta Arithmetica, LXXXIX.3, (1999), 259–277.
9. C. Ballot, *Counting monic irreducible polynomials P in $F_q[X]$ for which order of $X \pmod{P}$ is odd*, J. Théor. Nombres Bordeaux **19** (2007), no. 1, 41–58.
10. C. Ballot, *An elementary method to compute prime densities in $F_q[X]$*, Combinatorial number theory, 71–80, de Gruyter, Berlin, 2007.
11. C. Ballot, *Competing prime asymptotic densities in $F_q[X]$: a discussion*, Enseign. Math. (2) **54** (2008), no. 3-4, 303–327.
12. C. Ballot, *On the 1/3 density of odd ranked primes in Lucas sequences*, Unif. Distrib. Theory **3** (2008), no. 2, 129–145.

13. C. Ballot, *Lucas sequences with cyclotomic root field*, Dissertationes Math. **490** (2013), 92 pp.
14. C. Ballot and M. Elia, *Rank and period of primes in the Fibonacci sequence. A trichotomy*, Fibonacci Quart. **45** (2007), no. 1, 56–63.
15. C. Ballot and F. Luca, *Prime factors of* $a^{f(n)} - 1$ *with an irreducible polynomial* $f(x)$, New York J. Math. **12** (2006), 39–45.
16. C. Ballot and F. Luca, *Common prime factors of* $a^n - b$ *and* $c^n - d$, Unif. Distrib. Theory **2** (2007), no. 2, 19–34.
17. E. Bavencoffe, *PPCM de suites récurrentes linéaires*, C. R. Acad. Sci. Paris Sér. I Math. **318** (1994), no. 9, 791–794.
18. A. Berger and T. Hill, *A basic theory of Benford's law*, Probab. Surv. **8** (2011), 1-126.
19. Arno Berger and Theodore Hill, *An Introduction to Benford's Law*, Princeton University Press, Princeton, NJ, 2015. viii+248 pp.
20. J.-P. Bézivin, *Plus petit commun multiple des termes consécutifs d'une suite récurrente linéaire*, (French) [Least common multiple of the consecutive terms of a linear recurrence sequence] Collect. Math. **40** (1989), no. 1, 1–11 (1990).
21. H. Bilharz, *Primdivisoren mit vorgegebener Primitivwurzel*, (German) Math. Ann. 114 (1937), no. 1, 476–492.
22. A. Brauer, *A note on a number theoretical paper of Sierpiński*, Proc. Amer. Math. Soc. **11** (1960), 406–409.
23. J. Brillhart, *Note on representing a prime as sum of two squares*, Math. Comp. **26** (1972), 1011–1013.
24. P. Bruckman and P. Anderson, *Conjectures on the Z-densities of the Fibonacci sequence*, Fibonacci Quart. **36** (1998), no. 3, 263–271.
25. P. Cubre and J. Rouse, *Divisibility properties of the Fibonacci entry point*, Proc. Amer. Math. Soc. **142** (2014), no. 11, 3771–3785.
26. Graham Everest, Alf van der Poorten, Igor Shparlinski, Thomas Ward, *Recurrence Sequences*, Mathematical Surveys and Monographs **104**, Amer. Math. Soc., Providence, RI, 2003.
27. A. Fuchs and G. Letta, *Le problème du premier chiffre décimal pour les nombres premiers* (French) [The first digit problem for primes] The Foata Festschrift. Electron. J. Combin. **3** (1996), no. 2, Research Paper 25, approx. 7 pp.
28. P. X. Gallagher, *The large sieve and probabilistic Galois theory*, Proceedings of symposia in pure mathematics, **24** (1973), 91–101.
29. A. Granville and G. Martin, *Prime number races*, Amer. Math. Monthly **113** (2006), no. 1, 1–33.
30. H. Hasse, *Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl* $a \neq 0$ *von gerader bzw. ungerader Ordnung mod.p ist*, Math. Ann. **166** (1966), 19–23.
31. H. Hasse, *Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl* $a \neq 0$ *von durch eine vorgegebene Primzahl* $l \neq 2$ *teilbarer bzw. unteilbarer Ordnung mod.p ist*, Math. Ann. **162** (1965/66), 74–76.

32. C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.
33. P. Kiss and F. Mátyás, *An asymptotic formula for* π, J. Number Theory **31** (1989), no. 3, 255–259.
34. L. Kronecker, *Über die Irreductibilität von Gleichungen*, Monatsb. König. Preuss. Akad. Wiss. Berlin (1880), 155–162.
35. J. Lagarias, *The set of primes dividing the Lucas numbers has density 2/3*, Pacific J. Math. **118**, 2 (1985), 449–461; Errata: Pacific J. Math. **162**, (1994), 393–397.
36. Michaël Launay, *Le Théorème du Parapluie*, Editions Flammarion, 2019.
37. R. Laxton, *On groups of linear recurrences I*, Duke Math. J. **26** (1969), 721–736.
38. R. Laxton, *On groups of linear recurrences II. Elements of finite order*, Pacific J. Math. **32** (1970), 173–179.
39. Ž. Ljujić, *Prime densities for generalized Lucas sequences*, Master's Thesis, University of Leiden, 2007, available at https://algant.eu/documents/theses/ljujic.pdf
40. Daniel Marcus, *Number Fields*, Universitext Springer-Verlag, New York-Heidelberg, 1977. viii+279 pp.
41. Y. Matiyasevich and R. Guy, *A new formula for* π, Amer. Math. Monthly **93** (1986), no. 8, 631–635.
42. P. Moree, *On the prime density of Lucas sequences*, J. Théor. Nombres Bordeaux **8** (1996), no. 2, 449–459.
43. P. Moree, *On primes p for which d divides* $ord_p(g)$, Funct. Approx. Comment. Math. **33** (2005), 85–95.
44. P. Moree and P. Stevenhagen, *Prime divisors of Lucas sequences*, Acta Arith. **82** (1997), no. 4, 403–410.
45. P. Moree and P. Stevenhagen, *A two-variable Artin conjecture*, J. Number Theory **85** (2000), no. 2, 291–304.
46. P. Moree and P. Stevenhagen, *Prime divisors of the Lagarias sequence*, 21st Journées Arithmétiques (Rome, 2001). J. Théor. Nombres Bordeaux **13** (2001), no. 1, 241–251.
47. P. Morton, *Musings on the prime divisors of arithmetic sequences*, Amer. Math. Monthly **97** (1990), no. 4, 323–328.
48. S. Müller, *On the rank of appearance and the number of zeros of the Lucas sequences over* $\mathbb{F}_q$, Finite fields and applications (Augsburg, 1999), 390–408, Springer, Berlin, 2001.
49. L. Murata, *On certain densities of sets of primes*, Proc. Japan Acad. Ser. A Math. Sci. **56** (1980), no. 7, 351–353.
50. L. Murata, *On some fundamental relations among certain asymptotic densities*, Math. Rep. Toyama Univ. **4** (1981), 47–61.
51. W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, PWN-Polish Scientific Publishers, Warsaw, 1974.
52. F. Pappalardi, *Square free values of the order function*, New York J. Math. **9** (2003), 331–344.

53. Harry Pollard, *The Theory of Algebraic Numbers*, Carus Monograph Series, no. 9. Mathematical Association of America, Buffalo, N.Y., 1950. xii+143 pp.
54. G. Pólya, *Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen*, (German) J. Reine Angew. Math. **151** (1921), 1–31.
55. K. Prachar, *Primzahlverteilung*, Springer-Verlag, 1957.
56. R. Robinson, *A report on primes of the form* $k2^n + 1$ *and on factors of Fermat numbers*, Proc. Amer. Math. Soc. **9** (1958), 673–681.
57. Michael Rosen, *Number theory in Function Fields*, Graduate Texts in Mathematics, 210. Springer-Verlag, New York, 2002. xii+358 pp.
58. Joseph J. Rotman, *An Introduction to the Theory of Groups*, Wm. C. Brown Publishers, Dubuque, Iowa, third edition, 1988.
59. C. Sanna, *On the divisibility of the rank of a Lucas sequence*, (2020), available at https://arxiv.org/abs/2008.12506
60. A. Schinzel, *On the linear dependence of roots*, Acta Arithmetica **28**, (1975), 161–175.
61. Jean-Pierre Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics, 7, Springer-Verlag, New York-Heidelberg, 1973.
62. D. Shanks, *Fibonacci primitive roots*, Fibonacci Quart. **10** (1972), no. 2, 163–168, 181.
63. D. Shanks, *Proof of Krishnamurthy's conjecture*, J. Recreational Math. **6** (1973), no. 1, 78–79.
64. Daniel Shanks, *Solved and Unsolved Problems in Number Theory*, Chelsea Publishing Company, New York, N. Y. 4th edition, 1993.
65. W. Sierpiński, *Sur une décomposition des nombres premiers en deux classes*, (French) Collect. Math. **10** (1958), 81–83.
66. L. Somer, *Linear recurrences having almost all primes as maximal divisors*, Fibonacci numbers and their applications (Patras, 1984), 257–272, Math. Appl., 28, Reidel, Dordrecht, 1986.
67. P. J. Stephens, *Prime divisors of second-order linear recurrences*, I. J. Number Theory **8** (1976), no. 3, 313–332.
68. P. Stevenhagen and H. W. Lenstra, *Chebotarëv and his density theorem*, Math. Intelligencer **18** (1996), no. 2, 26–37.
69. N. Suwa, *Geometric aspects of Lucas sequences, I*, Tokyo J. Math. **43** (2020), no. 1, 75–136.
70. N. Suwa, *Geometric aspects of Lucas sequences, II*, Tokyo J. Math. **43** (2020), no. 2, 383–454.
71. N. Suwa, *Geometric aspects of Lucas sequences, a survey*, Algebraic Number Theory and Related Topics 2018, 149–176, RIMS Kôkyûroku Bessatsu, B86, Res. Inst. Math. Sci. (RIMS), Kyoto, 2021.
72. N. Suwa, *Geometric aspects of Cullen-Ballot sequences*, preprint (submitted to the Pacific J. Math. Nov. 20th, 2019).
73. N. Tschebotareff (= N. G. Chebotarëv), *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehren*, Math. Ann. **95** (1925), 191–228.

74. J. Vinson, *The relation of the period modulo to the rank of apparition of m in the Fibonacci sequence*, Fibonacci Quart. **1** (1963), no. 2, 37–45.
75. B. L. van der Waerden, *Algebra*, Volume I, Springer-Verlag, New York, Inc., seventh edition, 1991.
76. M. Ward, *The null divisors of linear recurring series*, Duke Math. J. **2** (1936), 472–476.
77. M. Ward, *Prime divisors of second order linear recurrences*, Duke Math. J. **21** (1954), 607–614.
78. M. Ward, *The maximal prime divisors of linear recurrences*, Canadian J. Math. **6** (1954), 455–462.
79. M. Ward, *The prime divisors of Fibonacci numbers*, Pacific J. Math. **11** (1961), 379–386.
80. K. Wiertelak, *On the density of some sets of primes*, I and II. Acta Arith. 34 (1977/78), no. 3, 183–196, 197–210.
81. H. C. Williams, *A Generalization of the Lucas Functions*, Ph. D. Thesis, University of Waterloo, 1969.
82. H. C. Williams, *Some properties of a special set of recurring sequences*, Pacific J. Math. **77**, no. 1, (1978), 273–285.

Chapter 10
Epilogue and Open Problems

Study hard what interests you the most in the most undisciplined, irreverent and original manner possible. (Richard Feynman)

Il passa sa licence à la faculté des sciences de Montpellier, sans que ses professeurs le remarquent (ni du reste qu'il remarque ses professeurs). (Laurent Schwartz à propos de Grothendieck)

Abstract We conclude with a brief review of the topics introduced in this book and Lucas' connection to them. This is followed by an eclectic assortment of unsolved problems.

10.1 Epilogue

As we have seen in Chap. 1, Lucas claimed that a reason for his development of the theory of his sequences was their possible utilization in a proof of Fermat's last theorem. Undoubtedly, this played a significant role in his interest in these sequences, but his own work strongly suggests that the main impetus for this research evolved from his fascination with the Fibonacci sequence. The progression of his papers clearly displays how his discovery of the properties of the Lucas sequences developed from his empirical study of the Fibonacci numbers. He summarized much of this work in the first part of [9] and more extensively in his memoir [10], the main body of which appears in a substantially extended and revised form in Chap. 2, which is devoted to a number of basic results concerning the Lucas sequences—some of these were known to Lucas, but many were not. Indeed, this entire book can be considered as a greatly expanded version of [10].

At the beginning of his inquiries, Lucas was particularly interested in how the theory of his sequences could be applied to the problem of primality

© Springer Nature Switzerland AG 2023

C. J.-C. Ballot, H. C. Williams, *The Lucas Sequences*, CMS/CAIMS Books in Mathematics 8, https://doi.org/10.1007/978-3-031-37238-4_10

testing, particularly to the Mersenne numbers. Later, he extended these ideas to numbers of the form $Ap^n \pm 1$, where p is a prime. This is discussed in some detail in Chap. 3, as are a number of other applications of his sequences, extending even to cryptography. In view of Lucas' interest in this subject [17, Sect. 15.3], he would likely have found this development very gratifying.

As mentioned in Sect. 4.1, Lucas discovered the connection between his sequences and the circular and hyperbolic trigonometric functions. This is discussed at greater length in Chap. 4 (and Chap. 6) as are several other features of his sequences. In particular, we provide a correct proof of his Fundamental theorem in Sect. 4.3. On p. 291 of [10], he introduced the concept of a proper divisor of (U_n). This is a prime which divides some U_n, but does not divide U_m for any positive $m < n$. This, of course, is what we call a primitive divisor today. Lucas believed that if $D > 0$ and n is sufficiently large, then U_n would possess at least one primitive divisor, but as we saw in Sect. 4.5, it wasn't until much later that Carmichael was able to prove this. In his attempt to extend some of Lucas' tests for the primality of Mersenne numbers to exponents of the form $4k + 1$, Lehmer was frustrated by the fact that D cannot be 2 or 3 modulo 4; this caused him to devise what are today called the Lehmer sequences. These sequences are defined and some of their properties are given in Sects. 4.4 and 5.9.

As we mentioned at the beginning of Sect. 5.2, Lucas [10] did not introduce the Lucasnomials, but made the fundamental observation that makes these objects integers, i.e., he showed why the product of the first n terms $U_1 \cdots U_n$ of a regular Lucas sequence divides the product of any n consecutive terms of the sequence. He did not make any other substantial contribution to their study. Chapter 5 is concerned with the enormous number of developments concerning Lucasnomials, which, omitting work on q-binomials, should have started with Ward's paper [15] of 1936, but really started with Gould [6] in 1969. Lucasnomials, which are a nontrivial generalization of ordinary binomial coefficients, surprisingly share extended versions of various classical arithmetic properties of binomial coefficients. One of these properties, Lucas' congruence, which is the object of Sect. 5.7, was actually discovered by Lucas himself. Other surprises are an extended rule of Kummer that determines their p-adic valuation and various forms of the famous Wolstenholme congruence modulo the square or the cube of a prime treated in Sect. 5.8.

In Chaps. 6, 7, and 8, we dealt at some length with the problem of generalizing the Lucas sequences. As discussed in Sect. 6.1, this problem was of great interest to Lucas, and certain aspects of it were examined in [10], but for several possible reasons, Lucas never made much headway into its solution. We now know of several different possible extensions or generalizations, depending upon what it was that Lucas might have considered to be appropriate. In Chap. 6 we dealt with Lucas' conviction that an extension of his sequences might be found by considering linear recurring sequences of order three or sequences of symmetric functions of the zeros of cubic polynomials. In Chap. 7, we examined the application of linear recurrences of degree

greater than three to this problem. Also, the Lehmer functions were generalized, culminating in an algorithm which is both necessary and sufficient for establishing the primality of $Ap^n \pm 1$, where p is a prime. As it appears that divisibility sequences played an important role in Lucas' thinking, Chap. 8 is dedicated to the application of a few types of these sequences, including elliptic divisibility sequences and certain linear divisibility sequences, to the generalization problem.

Finally, in Chap. 9 we looked at an aspect of another problem that Lucas considered: the structure of the set of prime divisors of the terms of the (U_n) sequence. We studied this earlier in Chap. 2 and to some degree in Sect. 4.3, but here the emphasis is on the existence and determination of the density of the primes that divide the terms of the (V_n) sequence. For example, the density of the primes that divide the terms of the sequence (L_n) is $2/3$. In Chap. 9, we also discussed several directions in which the techniques of Hasse and Lagarias for proving the prime density of the (V_n) sequences could be extended. For instance, one direction seeks asymptotics for the sets of primes whose rank in a given Lucas sequence $U(P, Q)$ is divisible by a fixed integer $m \geq 2$. Another consists of discovering special cubic recurrences where primes that divide two consecutive terms of the recurrence have a density that can be computed unconditionally. Yet another direction sought a notion of "prime" natural density in polynomial rings over finite fields which allows analogous work. This density calculation was carried out successfully at least for the polynomial companion Lucas sequence $(X^n + 1)_{n\geq 0}$ in all such rings.

We have seen, then, that much has been learned about the Lucas sequences since the end of the nineteenth century. Indeed, it seems remarkable that such a large amount of activity has been devoted to such a simple pair of sequences, but still there seems to be much more to do. A glance at publications such as the *Journal of Integer Sequences*, the *Fibonacci Quarterly*, *Integers*, and the *Online Encyclopedia of Integer Sequences* (OEIS) suggests that interest in these sequences shows no sign of diminishing.

10.2 Some Unsolved Problems

In the course of writing this book, the authors encountered some problems concerning the Lucas sequences or their possible generalizations that are of some interest (at least to us) and remain unsolved or unexplored. Naturally, a collection of such problems, reflecting the interests of the authors, is both eclectic and idiosyncratic, but it is our hope that bringing them to the readers' attention may stimulate further research. We have resisted the temptation to include questions that, while related to certain Lucas sequences, are well studied and still remain unanswered; for example, the Lucas sequence $(U_n(3, 2))$ is the Mersenne sequence, concerning which there are many well-known mysteries.

1. *Fibonacci-Wieferich primes.* From results in Chap. 2, it is easy to see that a prime p ($\neq 5$) will always divide $U_{p-\epsilon}(1,-1) = F_{p-\epsilon}$, where $\epsilon = 1$ when $p \equiv \pm 1 \pmod 5$ and $\epsilon = -1$, otherwise. The question is: does p^2 ever divide $F_{p-\epsilon}$? The Wall-Sun-Sun conjecture mentioned in Remark 12 suggests that the answer is no. Such a prime is called a Fibonacci-Wieferich prime. A computer search over all primes less than 2×10^{14} conducted by McIntosh and Roettger [11] was unsuccessful in finding such a prime, and the question remains as to their existence. The authors of [11] give some statistical reasoning to suggest that Fibonacci-Wieferich primes might exist, but this kind of argument, while seemingly reasonable, does not take into account aspects of the structure of the Fibonacci numbers. See, for example, Williams [16]. This suggests the additional problem of investigating the properties of other Lucas-Wieferich primes.

2. *Common prime divisors of two companion Lucas sequences.* We have discussed in Chaps. 2 and 9 the prime divisors of $V_n(P,Q)$. Suppose we have two such sequences: $(V_n(P_1,Q_1))$ and $(V_n(P_2,Q_2))$. Show that if D_1D_2 is not a perfect integral square ($D_i = P_i^2 - 4Q_i$ for $i = 1,2$), then there must exist some $n > 0$ and an odd prime p such that $p \mid V_n(P_1,Q_1)$ and $p \nmid V_n(P_2,Q_2)$. Notice that if this is so, then we cannot have

$$V_n(P_1,Q_1) \mid 2V_n(P_2,Q_2) \text{ for all } n > 0.$$

The ideas in Chap. 9 can be used to explore many instances of this problem, but a complete answer to this question is still unknown.

3. *pth power nonresidues.* This problem concerns the primality testing algorithms presented in Chaps. 3 and 7 for $N_n = Ap^n + \gamma$, where $\gamma = \pm 1$, p is a fixed prime, A is a fixed integer and $p \nmid A$. When N_n is not a perfect pth power, does there exist an efficient algorithm for finding a prime q such that $q \equiv 1 \pmod p$ and $N_n^{(q-1)/p} \not\equiv 1 \pmod q$? This question was discussed at some length in Sect. 16.4 of [17] and in [14]. It appears that such an algorithm might exist, but none is known which can deal effectively with all values of N_n.

4. *Solution of $G_s(x) \equiv 0 \pmod r$.* This is another problem that arises in connection with primality testing of integers of the form N_n in Problem **3**. It is well known that if p is an odd prime, $s = (p-1)/2$, and $r \equiv \gamma \pmod p$ is also a prime, then the congruence

$$G_s(x) \equiv 0 \pmod r$$

has s distinct solutions (when $\gamma = 1$, the congruence holds for $x \equiv g + g^{-1}$, where g is any primitive root of r; when $\gamma = -1$, see, for example, Theorem 9.4.3 of [17]). Is it possible to characterize all the values of r for which there is an efficient polynomial time algorithm for solving

this congruence? Some aspects of this problem are briefly discussed in Sects. 9.4 and 11.3 of [17], but much about it remains unknown. Of course, there is such an algorithm if we have a fast method for finding a generator of the multiplicative group of the elements of the finite field $\mathbb{F}_q$, where $q = r$ when $\gamma = 1$ and $q = r^2$ when $\gamma = -1$; however, while it may be possible to do this for certain values of r, a general technique is not known and might not even exist. Several features of this problem, particularly when $\gamma = 1$, are discussed in Moree's extensive expository paper [13] on Artin's primitive root conjecture.

5. *Absolute pseudoprimes which are also absolute Lucas D-pseudoprimes.* This problem was mentioned at the end of Sect. 4.3. Do there exist any N and D such that $(D \mid N) = \epsilon(N) = -1$ and N is both a Carmichael number and an absolute Lucas D-pseudoprime? As mentioned in Sect. 4.3, such values of N must be the product of an odd number of distinct primes p satisfying $p - 1 \mid N - 1$ and $p + 1 \mid N + 1$.

6. *Linear divisibility sequences of order three.* The following problem is motivated by the discussion in Sect. 6.2. Classify all the third-order, nondegenerate LDSs (X_n). We know that there are no (X_n) when the characteristic polynomial $f(x)$ of (X_n) is irreducible, but what about the other two cases? Hall thought that Ward had disposed of one of these cases, but as we mentioned, there doesn't seem to be much evidence in support of this. In this case we have $f(x) = (x - r)(x^2 - sx + t)$, where r, s, t are integers and $x^2 - sx + t$ is irreducible; we have $f(x) = x^3 - Px^2 + Qx - R$, where $P = r + s$, $Q = rs + t$ and $R = rt$. It is then easy to verify that $X_n = U_n(s, t)$ satisfies the third-order linear recurrence:

$$X_{n+3} = PX_{n+2} - QX_{n+1} + RX_n, \tag{10.1}$$

but this (X_n) is of order *two*. Suppose that (X_n) is not a Lucas sequence as above. By using Hall's [8] method, it can be shown that if (X_n) is a divisibility sequence, is nondegenerate, and satisfies (10.1), then $s \neq 2r$ and $X_n = (2r^n - U_n(s, t))/(2r - s)$. If $t = r^2$, we must have $Q/P = r$, and if we put $w = P + r = 2r + s$, it is not difficult to verify that X_n must be $U_n(\sqrt{w}, r)^2$. Notice that $U_n(\sqrt{w}, r)^2$ is essentially the square of a Lehmer function (see Sect. 4.5), and the corresponding sequence is a divisibility sequence satisfying (10.1). If $t \neq r^2$, then it seems that there are no divisibility sequences satisfying our conditions, but this remains to be proved. Very little is known about the case when $f(x)$ is the product of three distinct linear polynomials.

7. *Linear divisibility sequences of order four.* We have seen in Sect. 8.3 that if (X_n) is a nondegenerate LDS of degree *four*, then its characteristic polynomial must be of the form:

$$f(x) = x^4 - Px^3 + (R + 2Q)x^2 - PQx + Q^2,$$

for some integers P, Q, R. The problem is that of determining all the LDSs with characteristic polynomial given by $f(x)$. In Sect. 8.5 we pointed out that there is always one and only one even LDS of order four with characteristic polynomial $f(x)$: the standard sequence. Put $\Delta = P^2 - 4R$ and $E = (R+4Q)^2 - 4QP^2$ and let $\Delta = Su^2$ and $E = Gv^2$, where S, G, u, v are integers and S and G are both square-free. It was shown in [19] that this problem has been solved for all odd sequences unless

$$\begin{aligned} &(a) \quad G = 1,\ S \neq 1, \\ &(b) \quad G = S \neq 1, \\ &(c) \quad G = S = 1. \end{aligned}$$

In Case (a), it is strongly suspected that no such sequence exists. By results in [19], this would be true if Problem **2** is ever solved. An extensive computer search did not uncover any odd nondegenerate LDSs when Case (b) holds. Indeed, if we make use of the notation and results in Sect. 7 of [18], it can be proved that a necessary and sufficient condition for A_2 to be an integer is that $(X/e) \mid H$, where $H = \gcd(u, v)$ and $e = \gcd(Y, 2T)$. By making use of this result, we can narrow down the possible instances of Case (b) where we get a nondegenerate odd LDS. In fact, it can be shown by a lengthy, but elementary, argument that there cannot be any if $\Delta = E$. When Case (c) holds, we have seen in Sect. 8.5 that there are many odd LDSs. The question in this case is: have we characterized all of them?

8. *Classification of all linear divisibility sequences.* Problems **6** and **7** are subproblems of this more general problem: for a given $k > 2$, is there a scheme which can be used to find all the LDSs of order k? This seems to be a very deep and difficult question. Certainly, it seems difficult for just $k = 3$ or 4. The only general tool currently available is Theorem 125, but this is not sufficient for solving the problem. What is needed is a result like Conjecture 126, but this has not yet been proved, and as pointed out in Sect. 8.3, there are difficulties in applying it.

Note added. It seems that very recently, Andrew Granville [7] has completely solved this problem. For example, as a consequence of this investigation, he can show that the only nondegenerate LDS of order three must be either $(n^2 a^{n-1})$, where a is an integer, or (U_n^2), where $U_n = U_n(\sqrt{w}, r)$ as in Problem **6**, is some Lucas or Lehmer function, thereby providing a complete solution of Problem **6**. This is a most remarkable solution to a long-standing problem, but the reader should be cautioned that, while the conclusions the author derives in [7] are easily understood, the techniques employed are very deep and well outside the scope of this book.

While [7] has yet to complete the peer review process, the ideas presented are convincing, and with inevitable minor corrections, the paper will very likely be accepted for publication.

9. *Lehmer sequences.* These were introduced in Sect. 4.4.

Using the Lehmer sequence $\bar{U} = \bar{U}(R, Q)$, which is a strong divisibility sequence (if $\gcd(R, Q) = 1$) and a fourth-order linear recurrence, we may consider the Lehmernomial coefficients

$$\binom{m}{n}_{\bar{U}},$$

defined in analogy with Lucasnomials. As we saw in Sect. 5.9, they are integers. We also saw that *Lehmernomial Catalan numbers*

$$\bar{U}_{n+1}^{-1}\binom{2n}{n}_{\bar{U}},$$

are always integers and Lehmernomial Fuss-Catalan numbers are too. All questions about Lucasnomials covered in Chap. 5 would need to be explored in the context of Lehmernomials, in particular finding out a combinatorial interpretation for Lehmernomials and Lehmernomial Catalan numbers, finding out a generalized Legendre formula, discovering a Kummer rule, evaluating their p-adic valuation, finding out whether they satisfy an extended Lucas congruence and some versions of the Wolstenholme theorems. We ask a few questions in a more precise manner.

(i) In Sect. 5.5.4, we saw that all Catalan-like triples (U, a, k), i.e., such that the numbers

$$\frac{1}{U_{(a-1)n+k}}\binom{an}{n}_{U},$$

are integers for all $n \geq 0$, have been discovered. The complete classification [5] of ℓ-defective Lucas sequences was one of the major tools that allowed this search to be successful, but the same paper [5] also includes the classification of ℓ-defective Lehmer sequences. Thus, the problem: find all Catalan-like triples $(\bar{U}, a, k)$, i.e., such that

$$\frac{1}{\bar{U}_{(a-1)n+k}}\binom{an}{n}_{\bar{U}},$$

are integers for all $n \geq 0$.

(ii) To date, we are not aware that the prime density of any companion Lehmer sequence $\bar{V} = \bar{V}(R, Q)$ has ever been computed.[†] This should

[†] Even though this very question was asked by Alan Baker in 1994 at the end of a lecture of C. Ballot.

be feasible because the complementary set of primes is simply the set of prime divisors of the second-order linear recurrence $(\bar{U}_{2n+1}(R,Q))_{n\geq 0}$. Of course, the more general order problem, i.e., estimating the prime density of sets

$$\{p;\ m \mid \bar{\rho}(p)\},$$

where $m \geq 2$ is a fixed integer, $\bar{\rho}$ is the rank of p in the Lehmer sequence $\bar{U}(R,Q)$, is also awaiting investigation and might be more challenging.

(iii) Is there a Wolstenholme phenomenon for pairs of Lehmer sequences when p is a prime of maximal rank? That is, suppose the rank of p in $\bar{U}(R,Q)$ is $\rho = p - \epsilon\sigma$, where $\epsilon = (D \mid p)$, $D = R - 4Q$ and $\sigma = (R \mid p)$, would we find out that some sums

$$\sum_{n\in S} \frac{\bar{V}_n}{\bar{U}_n}$$

are $0 \pmod{p^2}$, for some sets S? Do Lehmernomials satisfy an analogue of either of the congruences (5.83) or (5.84), which are two generalizations to Lucasnomials of the classical Wolstenholme congruence (5.71)?

(iv) Is there an analogue to Theorem 88, the generalization of Lucas' congruence of Hu and Sun, for Lehmernomials?

(v) Is there a relevant analogue of the Laxton group associated with a quadratic polynomial $f(x) = x^2 - \sqrt{R}x + Q$, R, Q integers, in which the Lehmer sequences would play a central role, and such that its binary operation would preserve division by primes? (See Sect. 9.7.)

(vi) Develop properties of the polynomial Lehmer sequences in $\mathbb{F}_q[X]$ associated with $Y^2 - \sqrt{R}\,Y + Q$, where R and Q are in $\mathbb{F}_q[X]$.

10. *Divisibility sequences and Catalan numbers.* Is it true that for every strongly divisible integral sequence (X_n), the numbers

$$\frac{1}{X_{n+1}}\binom{2n}{n}_X, \tag{10.2}$$

are integral? More generally, which divisibility sequences satisfy (10.2)?[‡] If the first question has a positive answer, then we would have another rich collection of generalized Catalan numbers. Investigation of Fuss-Catalan and generalized Fuss-Catalan numbers in this abstract setting could then follow.

11. *Maximal divisors of cubic recurrences.* Several of the open problems we cite here were alluded to in Sect. 9.8.

[‡] A question along these lines was asked by an anonymous referee who reviewed [2].

(i) Let $f(x) = (x-1)(x^2-x-1) = x^3 - 2x^2 + 1$. Is it true that the only integral cubic linear recurrences in $F(f)$ with positive prime density of maximal divisors are shifts and/or rational multiples of either $(-1 + F_{n+1})$ or $(1+F_{n+1})$? Note that $(-1+F_{n+1})$ is the fundamental sequence with initial values $0, 0, 1$, whereas $[2, 2, 3] = 1 + F_{n+1}$ is torsion of order 2 in the generalized Laxton group and has density of maximal divisors $2/3$; see [1].

(ii) Complete the work, alluded to toward the end of Sect. 9.8, initiated by Ballot and Luca [3, 4], to prove, or disprove, that maximal prime divisors of non-torsion recurrences with characteristic polynomial $f(x) = (x - \alpha)(x - \beta)(x - \gamma)$, where α, β and γ are nonzero integers of distinct absolute values, have zero density.

(iii) Can one adapt, at least in some cases, the conditional argument Moree and Stevenhagen used in [12]—see Remark 44—for determining the prime density of the second-order non-torsion Lagarias sequence (denoted Y), to finding out the prime density of the maximal divisors of a typical non-torsion third-order linear recurrence $M = (M_n)$? Say for (M_n) defined by the recursion

$$M_{n+3} = 5M_{n+2} - 9M_{n+1} + 5M_n,$$

and the initial values $[1, -2, 1]$?

(iv) Given $f \in \mathbb{Z}[x]$ monic of degree ≥ 4, is there a relevant group structure, $G(f)$, with respect to maximal division, whenever f has exactly two double zeros, or, instead, a single zero of multiplicity 3?

(v) Suppose D is a positive integer, not a perfect cube, and (x_1, y_1, z_1) is a fundamental solution to the cubic Pell equation:

$$x^3 + Dy^3 + D^2z^3 - 3Dxyz = 1.$$

Put $\alpha = x_1 + \delta y_1 + \delta^2 z_1$, where $\delta = \sqrt[3]{D}$, and let β and γ be the algebraic conjugates of α. Define three integral sequences $X = (x_n)$, $Y = (y_n)$, $Z = (z_n)$ by

$$\alpha^n = x_n + y_n\delta + z_n\delta^2.$$

Besides the family of discriminants D of the form $M^3 \pm 1$ discussed in Sect. 9.8, can we find other families of discriminants for which X, Y, and Z are torsion recurrences in $G(f)$, where $f = (x - \alpha)(x - \beta)(x - \gamma)$? Assuming a positive answer, can we compute their prime density of maximal divisors? How often would the class of the sequence $(\alpha^n + \beta^n + \gamma^n)$ turn out to be of order *three* in the generalized Laxton group $G(f)$? Could its density of maximal divisors be evaluated?

(vi) Define a *primitive* prime maximal divisor of U_n, where $U = (U_n)$ is a fundamental recurrence with characteristic monic polynomial f in $\mathbb{Z}[x]$,

as a prime which is a maximal divisor of U at n, but is not a maximal divisor of U at any k, $0 < k < n$. Are there cubic recursions (with irrational roots) for which we can entirely describe the set Z of indices n for which there is a primitive prime maximal divisor of $U = [0, 0, 1]$ at n? If so, would there exist, for some of these recurrences, a positive integer N such that at least one of the two conditions (i) $\gcd(U_n, U_{n+1}) \leq N$, or (ii) $n \in Z$, holds for all $n \geq 1$?

(vii) Compute the density of primes P in $\mathbb{F}_q[X]$ which have an even rank $\rho_{\max}(P)$ of maximal division for the recursion defined by

$$(Y - X)(Y - X - 1)(Y - 1),$$

and initial values $0, 0$ and 1.
Can we use an elementary method which shows this set of primes has a d_3 density? (See Sects. 9.8 and 9.9.)

12. *Lucas theory in other rings than* $\mathbb{Z}$.

(i) Develop the theory of Lucas sequences $U(P, Q)$, $V(P, Q)$ in $\mathbb{F}_q[X]$ much in the way it is done in Chap. 2 of this book. Here P and Q are nonzero polynomials in $\mathbb{F}_q[X]$.

(ii) Would the study of the analogue of the Laxton group for second-order recurrences of polynomials in $\mathbb{F}_q[X]$, associated with the characteristic polynomials $Y^2 - PY + Q$, have features of interest?

(iii) Develop the basic theory of Lucas sequences, as in Chap. 2, in the rings of Gaussian integers $\mathbb{Z}[i]$, or Eisenstein integers $\mathbb{Z}[\omega]$, where $\omega = e^{2\pi i/3}$, or in rings of integers in general, but also in more esoteric rings such as Drinfeld modules, or the ring of Hurwitz quaternions, i.e., quaternions $a+bi+cj+dk$, where a, b, c, and d are all rational integers, or all halves of odd rational integers. Here, the three quaternions i, j, k satisfy the quaternionic relations $i^2 = j^2 = k^2 = ijk = -1$.

13. *Wolstenholme's phenomenon.* See the remarks made at the end of Sect. 5.8.

Find a common characterization for all pairs of second-order recurrences X and Y that share the same quadratic characteristic polynomial $x^2 - Px + Q \in \mathbb{Z}[x]$, and satisfy for all, but finitely many primes p of maximal rank, i.e., of rank p, or $p \pm 1$ (with respect to the Lucas sequence $U(P, Q)$), the congruence

$$\sum_I \frac{Y_n}{X_n} \equiv 0 \pmod{p^2},$$

on all intervals I of maximal length with respect to the condition $X_n \neq 0$.

References

1. C. Ballot, *The density of primes p, such that* -1 *is a residue modulo p of two consecutive Fibonacci numbers, is* $2/3$, Rocky Mountain J. Math. **29** (1999), no. 3, 749–761.
2. C. Ballot, *Divisibility of the middle Lucasnomial coefficient*, Fibonacci Quart. **55** (2017), no. 4, 297–308.
3. C. Ballot and F. Luca, *Prime factors of* $a^{f(n)} - 1$ *with an irreducible polynomial* $f(x)$, New York J. Math. **12** (2006), 39–45.
4. C. Ballot and F. Luca, *Common prime factors of* $a^n - b$ *and* $c^n - d$, Unif. Distrib. Theory **2** (2007), no. 2, 19–34.
5. Y. Bilu, G. Hanrot, P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, With an appendix by M. Mignotte, J. Reine Angew. Math. **539** (2001), 75–122.
6. H. W. Gould, *The bracket function and Fontené-Ward generalized binomial coefficients with application to Fibonomial coefficients*, Fibonacci Quart. **7** (1969) 23–40, 55.
7. A. Granville, *Classifying Linear Division Sequences*, https://arxiv.org/abs/2206.11823
8. M. Hall, *Divisibility sequences of the third order*, Amer. J. Math. **58** (1936), 577–584.
9. É. Lucas, *Sur la série récurrente de Fermat*, Bolletino di Bibliografia e di Storia della Scienze Matematiche e Fisiche **11** (1878), 783–789.
10. É. Lucas, *Théorie des fonctions simplement périodiques*, Amer. J. Math. **1** (1878), 184–240, 289–321.
11. R. J. McIntosh and E. L. Roettger, *A search for Fibonacci-Wieferich and Wolstenholme primes*, Math. Comp. **76** (2007), no. 260, 2087–2094.
12. P. Moree and P. Stevenhagen, *Prime divisors of the Lagarias sequence*, 21st Journées Arithmétiques (Rome, 2001). J. Théor. Nombres Bordeaux **13** (2001), no. 1, 241–251.
13. Pieter Moree, *Artin's primitive root conjecture–a survey*, Integers 12A (2012), #A13.
14. A. Stein and H. C. Williams, *Explicit primality criteria for* $(p-1)p^n - 1$, Math. Comp. **69** (2000), 1721–1734.
15. M. Ward, *A calculus of sequences*, Amer. J. Math. **58** (1936), no. 2, 255–266.
16. H. C. Williams, *A note on the Fibonacci quotient* $F_{p-\epsilon_p}$, Can. Math. Bull. **25** (1982), 366–370.
17. H. C. Williams, *Édouard Lucas and Primality Testing*, Canadian Math. Soc. Series of Monographs and Advanced Texts, John Wiley and Sons, NY, 1998.
18. H. C. Williams and R. K. Guy, *Some monoapparitic fourth order linear divisibility sequences*, Integers **12A** (2012), #A17.
19. H. C. Williams and R. K. Guy, *Odd and even divisibility sequences of order 4*, Integers **16** (2015), #A33.

Appendix: A Short Biography of Lucas with Comments on His Work and Scientific Legacy

Name the greatest of all inventors. Accident. (Mark Twain)

La chance ne sourit qu'aux esprits préparés. (Louis Pasteur)

In what follows we provide a brief biography of Lucas, along with, inevitably, our personal interpretations and commentaries. For more information concerning Lucas' life and career, and how to better understand it within the social and political context of the time, together with his rich interactions with several contemporaries, we refer the reader to several papers of the late Anne-Marie Décaillot and her coauthors [4, 6, 8, 9], and to her very detailed Ph.D. thesis [7]. The collection of obituaries published in [3] also contains some interesting material.

François Édouard Anatole Lucas was born on April 4, 1842, the eldest of a family of eight children in Amiens, France, an historic medium-size city situated some 115 km north of Paris. His father's trade was that of a cooper, which meant that his family was of modest financial means. His primary education took place at a local parochial elementary school (l'École des Frères). While there, he seems to have impressed his teachers as a very gifted child, and attracted the attention of Jacques Garnier (1808–1888), an active polymath, who taught mathematics at the Imperial Lycée[†] in Amiens. Garnier

[†] A lycée is a secondary school for pupils aged 14–18. The "Grandes Écoles," Selective National Schools, are a system of higher education parallel to the university system, which was mostly put in place during the French Revolution and Napoleonic times, and continued to evolve in the nineteenth century. Up to the present, young people have to compete and obtain the best ranks in order to get into these schools; preparatory years were put into place within the lycées. At the time of Lucas, some lycées offered a first preparatory year, called a class of elementary mathematics (*une classe de mathématiques élémentaires*) at the end of which students could compete for some schools (such as École navale or Saint-Cyr) or, enter a second preparatory year, called special mathematics ('une classe de mathématiques spéciales'), which mostly prepared students for the École Polytechnique

© Springer Nature Switzerland AG 2023

C. J.-C. Ballot, H. C. Williams, *The Lucas Sequences*, CMS/CAIMS Books in Mathematics 8, https://doi.org/10.1007/978-3-031-37238-4

recommended to the local council that Lucas be awarded a municipal bursary to attend the Lycée. He got a 3/4 bursary from 1856 to 1858, which, at the request of his father and because of his excellent academic grades, was transformed into a full bursary henceforth. Thus, Lucas was able to pursue a secondary education, first at the Imperial Lycée in Amiens, completed from 1859 to 1861 at the lycée in Douai, a city north of Amiens, in the northern part of France. In Douai he followed their special mathematics class in order to prepare for the contest for admission to the École Polytechnique and to the École Normale Supérieure (ENS). As was often the case, he did a second year of special mathematics. In fact, a waiver was required for him to compete for the ENS as he was too young at the end of his first year of special mathematics. It seems, from a remark of the headmaster at Douai, that people intended him to pursue his studies with the ENS, from where he would be trained as an excellent teacher, rather than the—at the time—more prestigious École Polytechnique. He was admitted in 1861 both to the École Polytechnique and to the École normale supérieure (ENS), which are still today two of the most prestigious postsecondary schools (Grandes Écoles) in France. He decided in favor of the ENS, a school which, to this day, allocates a monthly state bursary to each of its attendees. After graduating in 1864, he secured second place in the mathematical sciences component of the competitive examination (agrégation) conducted by the state for admission to posts on the teaching staff of the lycées and preparatory classes to the Grandes Écoles. Incidentally, the individual who scored first place was Gaston Darboux [6] (1842–1917), who went on to a stellar career in mathematics (geometry and analysis). As Lucas was not yet 25, his official nomination as agrégé (i.e., someone who had successfully passed the agrégation) was delayed.

Louis Pasteur, aware, as a number of personalities of the time, of the superiority of Germany over France in the sciences and the director for scientific studies at the ENS, did everything in his power to recruit and train excellent candidates who would both participate in the scientific life of France and provide a high-quality education for their students, noted *the inventive sagacity of Lucas in certain areas of mathematics*.

With the support of Pasteur[†] and at the request of Urbain Le Verrier, the Director of the Imperial Observatory in Paris, Lucas was attached to that establishment in September of 1864 with the title of Assistant Astronomer. Le Verrier was the famous astronomer who created great excitement in 1846 when he was able to discover and locate the planet Neptune *au bout de la plume* (i.e., at the tip of his pen) based on observed perturbations on the orbit of Uranus. Even if we know today that the glory associated with this discovery should have been shared with the British mathematician and

or the ENS, which had the same program. The vast majority of people admitted to the best schools did their preparatory years in Parisian lycées, but starting in the 1840s, a few provincial lycées had acquired a good reputation, as was the case of the lycée in Douai.

[†] From 1862 to 1866, 11 former students of the ENS were hired at the Imperial Observatory of Paris.

astronomer John Adams and that the calculations of Le Verrier were the object of later criticisms, one may understand that the young Lucas felt attracted by this opportunity. But the unpopularity of Le Verrier within the Observatory, especially in the late 1860s, is a well-established fact. Diverging views between Le Verrier and his collaborators created significant tension that grew stronger in late 1866. While Lucas' professional work at the observatory went well, at least during the first 2 years, he left his position in late 1869 after several stormy years of dealing with its Director, thus preceding the departure of a number of astronomers who resigned en masse early in 1870. Le Verrier's years of dictatorial methods of management created such turmoil that he finally ended up being dismissed from his position in February of 1870, shortly before the end of the Second Empire (Dec. 1852–Sep. 1870).

Much more information concerning Lucas' tenure at the Observatory can be found in [7], about why and in what conditions, he stayed there in spite of Le Verrier's wanting to fire him (and others) starting in late 1866. During this time, Lucas frequently sought out some escape from Le Verrier's bullying by investigating mathematical problems during periodic visits to Amiens. Through the work of another native of Amiens, Édouard Gand (1815–1891), he became familiar with the mathematics associated with industrial weaving. His work on this formed the subject of his first publication in 1867 and several subsequent papers. (See [7, Chap. 7] and [8] for further material concerning this.) Indeed, at the conclusion of his paper [16], Lucas suggests that the laws of the mathematics of weaving might be enlisted in the construction of a mechanism to verify the primality of Mersenne numbers.

Working at the Paris Observatory, in those days, involved a lot of routine work, which compounded with Le Verrier's lack of flexibility, would have tested the patience and the desire to serve well of many young scientists, especially those trained at the ENS. Indeed, the work of an astronomer, back then, was essentially calculatory and mathematical: the astronomer would carry out *by hand* the necessary calculations for the raw data reduction of the observation; astrophysics was not yet born. An interesting anecdote in regard to Le Verrier's attitude comes from Camille Flammarion's memoirs. Flammarion had been recruited at the Imperial Observatory in 1858 at the age of 16, and he recalled the strong negative reaction of Le Verrier when he shared with him his intention of seeing Neptune with a telescope. Le Verrier would never have sought to see for himself the planet he had discovered mathematically! Surely the ingenuity of Lucas and his strong desire to learn and improve would have stumbled against the rigidity of Le Verrier. But the long hours spent on calculations could only have sensitized Lucas toward the importance, in general, of imagining efficient procedures to abbreviate raw calculations and make them less daunting and tiresome. The interest of Lucas for the practical and algorithmic aspects of computing is evident in much of his work. His activities around the mechanization and automatization of procedures constituted one of his main lifelong centers of interest. We will come back to this later.

Lucas' career was interrupted by the July 19 outbreak of the Franco-Prussian War (1870–1871) in which he volunteered to serve in the Army of the Loire as an auxiliary lieutenant in the artillery. He took part, in particular, in the battles of Blois, Orléans, and Le Mans, served with distinction, being promoted to the rank of captain and was recommended twice for the Cross of the Legion of Honour, the greatest French order of merit for both military and civil service. During his military service, Lucas (see [20], XIV) conceived the problem of the "pile of cannonballs," a Diophantine problem in which the solver is to find the conditions under which a pile of cannonballs with a square base and organized as a square pyramid contains a number of cannonballs which is the square of an integer. Lucas conjectured that there could only be 1 or 4900 such cannonballs, a result that was finally proved by G. N. Watson in 1919. For more information concerning this problem, see Anglin [1]. This simply stated problem may have kindled Lucas' subsequent interest in Diophantine equations, for he deals at some length with such problems in [15] and [18].

On being discharged from the army, Lucas was faced with the problem of securing a teaching post. He was particularly interested in obtaining a position in Paris because he was working with Charles André (1842–1912) at the Imperial Observatory on a translation of Brünnow's treatise on spherical and practical astronomy. One volume of this translation had already appeared in 1870, and Lucas wished to be placed in a situation that would allow him to continue to work on the second volume. Lucas' contribution [20, VIII] was to revise the instructions and provide additional tables resulting from his calculations. Unfortunately, Lucas' request to be employed in Paris was turned down by the ministry, and instead he was appointed Professor of Special Mathematics (*mathématiques spéciales*) at the Lycée of Moulins, a provincial city some 300 km south of Paris, effective April of 1872. The second volume of the translation, with Lucas' contributions, appeared in 1872. It was during his stay in Moulins that he met and married Marthe Boyron (1852–1882), the orphaned daughter of a Parisian lawyer; they went on to have two children: Paul and Madeleine.

It seems that in Moulins, having been released from the turbulence and anxiety of the past several years, Lucas found the necessary serenity to pursue his mathematical interests. It was during this time that, very likely inspired by his interest in the Fibonacci sequence, he discovered the many properties of the Lucas sequences and applied these to the problem of the identification of large primes. Much more information concerning his contributions to primality testing can be found in Chap. 8 of [7] and in [26]. Suffice it to say that he was the first to recognize that certain large numbers could be proved prime, or composite, without recourse to a large number of trial divisions. We stress this was a fundamental and authentically novel discovery at the time, which today, as for many former fundamental discoveries, many of us take for granted. It is somewhat comparable to the invention of spectroscopy which brought about a qualitative denial to the philosopher Auguste Comte's claim

that we would never know the matter of which the stars are made because they were simply too far away. It was also during this time that Lucas made his first of many successive communications [17] to the French Association for the Advancement of Science (AFAS). In this work he mentioned once again, but without providing any detail, the possibility of constructing a machine to determine whether or not a Mersenne number is a prime.

As we said earlier, throughout his career Lucas was fascinated by the problem of mechanizing the process of computation. It may well be that he had always had an interest in this area of research, but it is also very possible that the appeal of this subject began as a result of his investigation into the application of weaving technology to number-theoretic problems. He wrote a lengthy essay [18] on calculation and calculating machines for the 1884 congress of AFAS in which he also introduced the work of Henri Genaille, a civil engineer working for the French railway, who was a very prolific inventor of calculating devices. This article was so admired that the first part of it was translated [19] into English for American readers. Lucas and Genaille also collaborated in the invention of several devices to simplify various common types of computation; these objects were reviewed with approbation in *Nouvelles Annales de Mathématiques* [2]. Later, he encouraged Genaille in his construction of the Arithmetic Piano, a device which could be used to reduce the labor needed in using Lucas' technique to verify the primality of Mersenne numbers. This instrument, which was described by Genaille to AFAS in 1891, is discussed in Sect. 7.2 of [26], in Chap. 12 of [7] and in [6]. Today there are 111 objects[†] associated with Lucas and 39 with Genaille in the *Conservatoire des Arts et Métiers* in Paris.

With respect to AFAS, Décaillot [8] has pointed out that it was first founded in 1872 to promote the interests of French science, and a few years later was used as a platform by a group of mathematicians whose ambition was to "contribute to the diffusion of science to a wide audience." To this end they dealt with mathematical questions that arose from concrete problems and made use of visual representations, particularly the chessboard. From 1876 until the year of his death, Lucas was a very active member of AFAS, rising to the level of Chair of the sections devoted to mathematics, astronomy, geodesy, and mechanisms.

Toward the end of his stay in Moulins, he submitted two theses to the Faculty of Science in Paris with the intention of being awarded a doctorate at Moulins in mathematical science. The subject matter of the first thesis ([20], XXIII) was geometry and of the second ([20], XXIV) was number theory—"the application of recurring series in the search for large prime numbers." Both theses were approved for defense by the Dean of the Faculty and received permission for printing, but Lucas did not bother to defend them. Possibly,

[†] i.e., $U_3(11, 10)$ ..., an impressive number at any rate, which reveals the popular interest for science and technological innovation in the years 1860–1880 in France as Décaillot mentions [7], as much as Lucas' involvement.

this was because his many pleas, since the conclusion of the war, for a position in Paris were finally being heard—he was offered a place in a Parisian lycée in the autumn of 1876. As this was the prize that Lucas was seeking, and as a doctorate at Moulins could only lead to a career in a provincial faculty, he likely felt that he should simply abandon this quest for a higher degree.

In September of 1876, Lucas was appointed professor at the Lycée Charlemagne, where he taught for two consecutive years a class of elementary mathematics until October of 1878; he then moved on to teaching a class of Special Mathematics, which covered the second part of the program for admission to the *Grandes Écoles*, from 1878 to 1879. He was rapidly promoted[†] to a professorial position at the Lycée Saint-Louis, where he commenced teaching Special Mathematics in October of 1879. He was granted an extended leave of absence from Saint-Louis for two school years (1882–1884) as a result of the death of his wife of 9 years. Nevertheless, he continued his mathematical activity during this time; indeed, he published the first two volumes of his mathematical recreations (*Récréations Mathématiques*) and devised the still popular game called the Tower of Hanoi, often used today as an example in explaining recursion to beginning computer science students. He first published this amusement under the pseudonym of N. Claus de Siam, an anagram of *Lucas d'Amiens*. For an extensive and well-researched discussion of the Tower of Hanoi, see Hinz et al. [12].

Lucas was described as a dynamic and enthusiastic man, who relished puns, a passionate scientist whose scholarship and manner charmed his audience. Through his various activities (recreational mathematics, the works of Fermat, the mechanization of computing, his personal research papers, etc.), he was in constant epistolary correspondence with many people. His research output was impressive, but his teaching performance at Saint-Louis became a source of conflict. It is difficult to imagine Lucas, a true fountain of ideas, quick to establish links between different areas of mathematics, being resistant to digressions, because they did not fit with the program of preparatory classes. But most students at Saint-Louis wanted to perform well at the national contests for which they were preparing. In 1890 Lucas' originality, and probable lack of rigor in covering the program, possibly due in part to the many projects he was involved with, led to a minor revolt of several students at Saint-Louis. They threatened to leave the lycée if they were assigned to his class because they thought that his teaching style would not adequately

[†] In the sense that there always was a tacit ranking of the lycées that prepared for the Grandes Écoles. The "better" lycées attracted both the better students and the better teachers. For instance, the headmaster of the Lycée Saint-Louis wrote [25] in his annual report of 1862: "M. Briot is known to be the best professor of all Parisian classes of special mathematics. His reputation is first-rate ..." A professor of mathematics who taught a class of "mathématiques spéciales" had only one class of students per year with about 15 hours per week of in-class mathematics and extra hours for oral quizzing of students in small groups, usually of three. There never was any reference manual. Each professor designed his own course and wrote it on the blackboard with students dutifully taking notes for hours on. In French slang, such a student is called *une taupe*, i.e., a mole.

prepare them for the competitive examinations. The result of this was a transfer of Lucas back to the Lycée Charlemagne in August of 1890, where he remained until his untimely death in the fall of 1891.

In 1891 Lucas completed the publication of his major work: *Théorie des Nombres* [23]. He had plans for publishing more volumes, but only the first volume ever appeared. This was the first book devoted to number theory to be published in France since the time of Legendre, almost 60 years earlier. Even though Lucas had some definite ideas for further material, it seems there were insufficient notes in his Nachlass for the production of any other volumes posthumously. (See [4], [7, Chap. 6], [11].) A charming and perceptive review of [23] was published in 1892 by Laisant† [13] shortly after Lucas' death. Décaillot, on the fourth page of the introduction of her thesis [7], gives an insightful description of this singular and very original book. Today, we would perhaps best summarize it by saying it is an idiosyncratic collection of topics in Discrete Mathematics, including elementary number theory, recurrences, graph theory, combinatorics, discrete probabilities, arithmetic devices, games, umbral calculus, the calculation of determinants, etc., nearly devoid of analytic methods.

Lucas' death came about as the result of a freak accident during an excursion in Provence, as part of the meeting of AFAS in Marseille (Sept. 18–28, 1891). While he was dining, a member of the serving personnel dropped a pile of plates behind Lucas' seat. A small piece of china flew up and caused a wound on Lucas' cheek. This wound bled copiously, but was not regarded at the time as being of much importance. On the way back to Paris, however, Lucas's cheek became inflamed and when he arrived home he took to his bed. He was diagnosed with erysipelas and died a few days later on October 3. Erysipelas is an illness of the upper dermis and by itself is rarely fatal, but one of its complications is necrotizing fasciitis (the so-called flesh-eating disease), which certainly answers to the description, *une courte et terrible maladie* supplied in the Forward of the third volume of *Récréations Mathématiques* [24], published posthumously in 1892. Lucas is buried in the Montmartre cemetery. (As reported by a mathematical friend, the tomb, in 1986, was in poor condition; Lucas' name and that of his daughter, Madeleine, were barely legible, due to moss on the horizontal stone. In 2015, it was a sad sight; the vertical limestone had broken into pieces gathered on the horizontal stone. It lies close to Jacques Offenbach's tomb.)

† Laisant (1841–1920) was an influential and very active personality and a close friend of Lucas with whom he shared mathematical interests and life experiences. He was a military officer, a parliamentary figure from 1876 to 1893, a freemason, meteorologist, mathematician (his 1877 Ph.D. thesis was on mechanical applications of the quaternions), a pedagogue, president of the SMF (*Société mathématique de France*) in 1888, director of the *Nouvelles Annales de Mathématique*, co-founder of mathematical journals, including *L'Enseignement Mathématiques*, still active today. He "used" his political position to promote Lucas on various occasions, e.g., as the head of a state-funded commission in charge of the reedition of Fermat's work.

During his relatively short career, Lucas wrote over 170 journal papers and 15 other documents such as books and sundry miscellaneous monographs. The subjects of these works spanned areas as varied as astronomy, mathematics of weaving, geometry, analysis, combinatorics, enumerative geometry, recurring sequences, recreational mathematics, and calculating devices; but his main interest seems to have been number theory, particularly Diophantine analysis. In retrospect, it seems that his most important impact on mathematics was the inspired work he did between 1875 and 1878 on primality testing. To get some idea of the extent and variety of Lucas' contributions, the reader is referred to Harkin's bibliography [11] and to the more complete compilation of Lucas' work at the website [14].

Unfortunately for Lucas, number theory was not in vogue in France during his lifetime; the subject was not taught in French universities, nor in the *Grandes Écoles*. Number theorists, except for Hermite and a few others, were essentially secondary school professors and members of scientific associations, such as the AFAS. (See [10].) Instead, the emphasis in French mathematics during that period was on analysis and geometry. The importance of analysis is obvious in military contexts; many of the Grandes Écoles, mainly in the first part of the nineteenth century, e.g., l'X,[†] were also military schools, partly due to the influence of Napoleon. Diligent and clever attempts by C.-A. Laisant to establish a Chair in number theory at the Collège de France,[‡] proposing Lucas as an obvious candidate, were met with opposition from the French mathematical establishment and were ultimately unsuccessful. In addition to this national bias, Lucas' use of elementary techniques, his emphasis on methods of computation, his delight in recreational mathematics, and his lack of an advanced degree likely united to ensure that he was relegated to the second tier of French mathematical scholarship. The effect of this was to cause his work to be largely ignored in France, until fairly recently. Perhaps it was this inattention which caused him to publish [20]. The name of Lucas in France was mostly associated with his books on recreational mathematics, and several of the games and themes they included.

His most important paper [19] was solicited by the English mathematician J. J. Sylvester (1814–1897) for publication in the USA, where it appears in the very first volume of the *American Journal of Mathematics*. Indeed, Sylvester was the inaugural Professor of Mathematics at Johns Hopkins University in Baltimore, on the East coast of the USA, at the time he founded this journal in 1878. He was a correspondent of the French Academy of Sciences in Paris, and took part in several meetings of the AFAS. Thus, he knew

[†] The French abbreviation for *l'École Polytechnique*.

[‡] A unique establishment situated in the Latin Quarter of Paris, formerly the Royal College, created by King Francis I in 1530, whose motto always was *omnia docet*, to teach every subject, and, in particular, subjects not taught in universities. Today it consists of about 50 chairs, awarded to individuals at the forefront of their subject, in all areas of the humanities, the sciences, or the arts, who carry on research and deliver free lectures. There is a website and online access to these lectures.

Lucas well. Lucas' creative memoir, with its theoretical, algorithmic, and calculatory aspects, and its numerous partial investigations got the attention fairly early of several American mathematicians such as E. T. Bell, D. N. Lehmer, R. D. Carmichael, D. H. and E. Lehmer, M. Ward, and others.

Bell (1883–1960), a prolific mathematician and writer, who occasionally wrote a science-fiction novel in 3 weeks, and the author of the influential book *Men of Mathematics*, was fascinated by the works of both Liouville and Lucas. The first volume of the *American Journal of Mathematics* was left missing from the Library at Stanford for a lengthy period: Bell had borrowed it and was staying in San Francisco in 1906 when the devastating earthquake occurred; the volume probably burned. As mentioned in Chap. 6 of this book, Lucas had envisioned a connection between Fermat's last theorem and the famous theorem of Jacobi concerning the impossibility of more than two periods for holomorphic functions of a single variable. In 1930, responding to a letter of Harkin on this subject, Bell wrote that he had "tried his darndest" to re-create this link for the last 28 years![†]

Morgan Ward (1901–1963) came to Pasadena where Bell was a faculty member at the California Institute of technology (Caltech) and actively participated in this quest. He published 33 articles on recurring sequences in his lifetime; many were influenced by Lucas' memoir and were often innovative and beautiful contributions. D. N. Lehmer (a friend of Bell) who taught mathematics at Berkeley from 1900 to 1937 and was the author of tables obtained by manual sieving (tables of factors; tables of prime numbers) transmitted to his son, D. H. Lehmer, the knowledge of Lucas and his taste for calculatory arithmetic and efficient algorithms. D. H. Lehmer (1905–1991), an influential figure of the twentieth century in number theory and in computational methods, had two mathematical heros: Ramanujan and Lucas. The title of his 1930 Ph.D. thesis was *An Extended Theory of Lucas' Functions*. Indeed, Lucas' seminal contributions regarding factoring and primality testing were not truly appreciated until the 1930s in the USA when D. H. Lehmer began the process of extending Lucas' research. This study, especially since the advent of public-key cryptography in the 1970s, has since been taken up by many academics around the world. For details concerning the history of these developments and many references, see [26]. D. H. Lehmer was a close friend of Ward.

Lehmer and his wife Emma initiated an informal gathering of number theorists on the eve of Christmas in 1969, which, today, has become an annual conference, the West Coast Number Theory Conference. At the end of the 1980s, it was a well-attended friendly meeting, typically attracting some 80 people. The Lehmers were often present; some former students of D. H. Lehmer (such as Brillhart, Graham, Stark, etc.), well-known or future well-known people were frequent participants, the likes of Bateman, Erdős, Granville, Lagarias, Odlyzko, Pomerance, Ribenboim, Selfridge, and many

[†] See Sect. 6.3.

more, as well as a number of graduate students. The name of Lucas was frequently heard, mostly in relation to primality testing or to his sequences, and it almost seemed as if he were a great-uncle, distant, but whose deeds were still being recounted.

Lucas' name is pervasive in both the written and oral communications of the *Fibonacci Association*. The Fibonacci Association, legally based in California, was founded by V. E. Hoggatt in 1962. Besides editing the *Fibonacci Quarterly*, it has overseen since 1984 the organization of an international conference on Fibonacci numbers that meets every 2 years, alternating the host institution between Northern or Central America, and Europe. Many of the talks involve the Lucas sequences, Fibonacci or Lucas numbers, and, more generally, linear recurrences or special integer sequences. All talks are contributed, but starting in 2008, the Association has invited a plenary speaker, called the *Lucas lecturer*, to its conference. The first Lucas lecturer was Carl Pomerance (Patras, Greece); to date, the last was Florian Luca (2022, Sarajevo, Bosnia-Herzegovina), and, along the way, in 2018, in Halifax, Canada, it was someone named Hugh Williams.[†] Marjorie Bicknell-Johnson who has been a member of the Association since its inception has written several papers on its history. (See [5], in particular; it contains a list of her other writings on this history.)

From a modern perspective, it is clear that Lucas was a pioneer in the study of efficient algorithms, particularly as they pertain to number theory and combinatorics; furthermore, in the pursuit of this activity, he was well ahead of his time. It is no exaggeration to regard him as a founder of the modern discipline of algorithmic number theory, and it is certainly appropriate that his name should be commemorated in the designation of the Lucas-Lehmer test for the primality of Mersenne numbers. In his hometown of Amiens, he is memorialized by having both a street (Rue Édouard Lucas) and a junior high school (Collège Édouard Lucas) named in his honor.

Lucas had undertaken for himself the mission of reviving the triple tradition coming from Fibonacci, Fermat (160x–1665)[‡], and Pascal (1623–1662), who, he wrote *were far-sighted, when today we are so short-sighted*. We recall that Pascal, in his youth, invented and supervised the manufacturing of what is often viewed as the first calculating machine, *La Pascaline*. Lucas might have added the tradition of recreational mathematics of Bachet (1581–1638), to which he greatly contributed with his four volumes of mathematical recreations. To him, these traditions went together and enriched each other. His curiosity and interest in the history of mathematics, especially in regard to the reedition of the collected works of Fermat, to which he contributed officially for a few years, should also be pointed out. (See [7, Chap. 11] for letters exchanged between the proponents of the project and the detailed and sometime chaotic events that surrounded this project.) In short, Lucas (Fig. 1)

[†] Hugh avers that he did not write this paragraph.

[‡] Where x is either 1, 5, 7, or possibly 8.

was able to pursue what he liked most, with passion and no doubt joy, in spite of several adverse circumstances, something which may be perceived as a definition of success.

Fig. 1 Édouard Lucas (1842–1891)

References

1. W. S. Anglin, *The square pyramid puzzle*, Amer. Math. Monthly **97** (1990), 120–194.
2. Anonymous, *Les appareils à calculs exacts et instantanés pour simplifier la multiplication et la division, inventés par Henri Genaille, et perfectionnés par M. Edouard Lucas*, Nouvelles Annales de Mathématiques **4**(3) (1885), 516–519.
3. Anonymous, *Notes sur M. Édouard Lucas Arithméticien*, Imprimerie Yvert et Tellier, Amiens, 1907.
4. J.-M. Autebert, A.-M. Décaillot and S. R. Schwer, *Henri-Auguste Delannoy et la publication des oeuvres posthumes d'Édouard Lucas*, Gaz. Math. No. **95** (2003), 50–62.
5. M. Bicknell-Johnson, *The Fibonacci Association: historical snapshots*, Fibonacci Quart. **52** (2014), no. 5, 1–4.

6. A.-M. Décaillot, *L'arithméticien Édouard Lucas (1842–1891): théorie et instrumentation* (French) [The arithmetician Édouard Lucas (1842–1891): theory and instrumentation] Rev. Histoire Math. **4** (1998), no. 2, 191–236.
7. A.-M. Décaillot, *Édouard Lucas (1842–1891): le parcours original d'un scientifique français dans le deuxième moitié du XIX-ième siècle*, Ph.D. Thesis, Université René Descartes-Paris V, 1999.
8. Anne-Marie Décaillot, *Géométrie des tissus. Mosaïques. Échiquiers. Mathématiques curieuses et utiles*, Rev. Histoire Math. **8** (2002), no. 2, 145–206.
9. Anne-Marie Décaillot, *Les Récréations mathématiques d'Édouard Lucas: quelques éclairages*, Historia Math. **41** (2014), no. 4, 506–517.
10. C. Goldstein, *La théorie des nombres dans les Notes aux Comptes Rendus de l'Académie des Sciences (1870–1914) : un premier examen*, Rivista di Storia della Scienza 1994, (S.II), **2** (2), 137–160.
11. D. Harkin, *On the mathematical work of François-Édouard-Anatole Lucas*, Enseign. Math. **3** (1957), 276–288.
12. Andreas M. Hinz, Sandi Klavžar and Ciril Petr, *The Tower of Hanoi–Myths and Maths*, Second Edition, Birkhäuser, Springer Nature, Cham Switzerland, 2018.
13. C.-A. Laisant, *Théorie des nombres*, Nouvelles Annales de Mathématiques, 3e série **11** (1892), 37–41.
14. Édouard Lucas website available at https://edouardlucas.free.fr
15. É. Lucas, *Recherches sur l'analyse indéterminée et arithmétique de Diophante*, Bulletin de la Société d'émulation du Département de l'Allier **12** (1873), 441–532.
16. É. Lucas, *Sur les rapports qui existent entre la théorie des nombres et le calcul intégral*, Comptes Rendus Acad. des Sciences, Paris **82** (1876), 1303–1305.
17. É. Lucas, *Sur la recherche des grands nombres premiers*, Assoc. Française pour l'Avancement des Sciences. Comptes Rendus **5** (1876), 61–68.
18. É. Lucas, *Recherches sur plusieurs ouvrages de Leonardo de Pise et sur diverses questions d'arithmétique supérieure*, Bolletino di Bibliographia e di Storia della Scienze Matematiche e Fisiche **10** (1877), 129–193, 239–293.
19. É. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. of Math. **1** (1878), 184–240, 289–321.
20. É. Lucas, *Notices sur les Titres et Travaux Scientifiques de M. Édouard Lucas*, D. Jouaust, Paris, 1880.
21. É. Lucas, *Le calcul et les machines à calculer*, Assoc. Française pour l'Avancement des Sciences. Comptes Rendus **13** (1884), 111–141.
22. É. Lucas, *Calculating machines*, Popular Science Monthly **26** (1884–85), 441–452.
23. É. Lucas, *Théorie des Nombres*, Éditions Jacques Gabay, Paris, 1991 (Authorized re-edition of the original 1891 Gauthier-Villars edition.)

24. É. Lucas, *Récréations Mathématiques*, T. III, Gauthiers-Villars, Paris, 2nd edition, 1893.
25. Hervé Renaud, *La fabrication d'un enseignement de l'analyse en France au XIXe siècle : acteurs, institutions, programmes et manuels*, Ph. D. Thesis, Université de Nantes, 2018, available at https://tel.archives-ouvertes.fr/tel-01699107
26. H. C. Williams, *Édouard Lucas and Primality Testing*, Canadian Math. Soc. Series of Monographs and Advanced Texts, John Wiley and Sons, NY, 1998.

Subject Index

Absolute Lucas D-pseudoprime, 91, 271
Addition formulas, 15
Algebraic integers, 224
Aliquot divisor of an integer, 53
Analytic density, 221
Artin symbol, 226
Artin's primitive root conjecture, 242
Associate Lucas sequence, 12
Aurifeuillian formula, 89

Base a pseudoprime (a-psp), 63
Bell's sequences, 173
Benford's law, 222
Binet forms, 13
Binomial theorem, 114
Bracelet tilings, 119
Brun's congruence, 152

Carlitz q-Catalan numbers, 128
Carmichael numbers, 58, 90, 271
Carmichael's theorem, 97
Catalan numbers, 125, 274
Catalan-like triples, 131, 273
Cebotarev density theorem, 219, 223, 226, 228, 260
Characteristic polynomial of a linear recurrence sequence, 184
Chebyshev polynomials, 82–86
Circular weighted tilings, 119
Companion Lehmer sequence, 273
Companion Lucas sequence, 12
Conjugacy class, 223
Cosine, 13, 79
Cryptography, 72
Cubic congruence, 65
Cubic linear recurrences, 171–172
Cubic Pell equation, 174–175, 257, 275
Cullen numbers, 253, 265
Cyclotomic polynomial, 70, 88–90

Decomposition group, 225
Defective, nondefective integer with respect to a sequence, 98
Degenerate (nondegenerate) Lucas sequences, 13, 44–45
Dickson polynomials, 85–86
Diophantine equation, 71
Dirichlet density, 221
Dirichlet density theorem, 224, 226
Discriminant, 13
Divisibility (divisible) sequence, 22
Divisibility polynomial, 205
Division polynomial of an elliptic curve, 203
Divisor set, 40

Elliptic curve, 203
Elliptic divisibility sequence (EDS), 202–204
Entry point, 27
Equivalent densities, 223
Euler's criterion, 42, 235
Euler's criterion for Lucas sequences, 42, 248
Euler's φ-function, 87
Even sequence, 212
Extended Lucas sequences, 208–212

Fermat congruence, 28, 58
Fermat's last theorem (FLT), 4, 166
Fibonacci numbers (sequence), 1–3, 6, 18, 30, 72, 93, 96, 139, 146, 152, 153, 245, 250, 267, 270, 288
Fibonomial Catalan numbers, 127
Fibonomials, 105
Frobenius automorphism, 29, 226
Frobenius density theorem, 223

© Springer Nature Switzerland AG 2023

C. J.-C. Ballot, H. C. Williams, *The Lucas Sequences*, CMS/CAIMS Books in Mathematics 8, https://doi.org/10.1007/978-3-031-37238-4

Frobenius map, 225
Fundamental Lucas sequence, 12
Fuss-Catalan numbers, 126

Galois field, 225
Galois group, 225, 228, 229, 232
Galois number field extension, 225
Gaussian or q-binomial coefficient, 14, 105, 123–143
Generalized binomial coefficients, 107
Generalized Laxton group, 251, 253, 254, 275
Generalized Legendre formula, 135, 137, 273
Generalized Lehmer sequences, 190–193, 211, 212
Generalized order problem, 252, 254
Girard-Waring formula, 20, 83

Hasse-Lagarias method, 237–240, 242, 250, 254, 258

Impulse response sequence, 187
Impulse sequences, 187
Inertial degree, 225
Integer factoring, 69–70
Iverson symbol, 12

Jacobi (elliptic) functions, 200, 201

Kronecker-Frobenius density theorem, 226, 238, 260
Kummer's rule, 133, 134
Kummer-Dedekind theorem, 227, 228, 238

Lagarias conditions, 239
Lagarias sequence, 242, 275
Lattice path, 119
Law of appearance, 28, 29
Law of regular division, 27
Law of repetition, 29, 193, 210
Laxton group, 157, 240, 245–250, 253, 274, 276
Legendre formula, 133
Lehmer sequences, 91–93, 97, 158, 183, 214, 268, 273
Lehmernomial Catalan numbers, 159
Lehmernomials, 158, 273, 274
Leonardo Bonacci, 2
Liber Abbaci, 2
Linear divisibility sequence (LDS), 204, 271
Linear recurrence sequences, 183–187
Logarithmic density, 221–223
Lucas functions, 12
Lucas numbers, 2, 3, 5, 6, 12, 35, 55, 153, 156, 234, 237, 243, 250, 288
Lucas pseudoprime, 63
Lucas sequences, 3
Lucas' congruence, 141–143
Lucas' fundamental theorem, 58, 87
Lucas-Lehmer test, 4, 57, 93, 288
Lucas-Wieferich prime, 270
Lucasian sequence, 205, 206, 248
Lucasnomial Catalan numbers, 125, 127, 128, 130
Lucasnomial Fuss-Catalan numbers, 127
Lucasnomials, 105
Lucaspolynomial, 108

Möbius function, 88
MacMahon q-Catalan numbers, 129
Maximal division, 274
Maximal divisor of a linear recurrence sequence, 251
Mersenne primes, 53
Minimal period length modulo m of a linear recurrence, 184
Modified Chebyshev polynomials, 83
Multinomial coefficient, 188
Multiplication formulas, 18–20, 83, 167, 170, 173, 174, 176, 178, 187, 188, 209, 210

n $\to U_n$ theme, 6
Natural density, 221
Non-null sequence, 184
Nondegenerate elliptic divisibility sequence, 202
Normalized divisibility sequence, 206
Null divisor of a linear recurrence sequence, 246
Number field, 224

Odd sequence, 212
Online Encyclopedia of Integer Sequences (OEIS), 203, 214, 215
Order (divisibility) problem, 240
Order of a linear recurrence sequence, 184

Parallel summation, 113
Pascal's identity, 112
Path weight, 119
Pell equation, 71, 82
Pell sequence, 35
Perfect number, 54
Period, 80
Perrin sequence, 170
Pierce sequences, 209
Pillai property, 6
Poncelet polygons, 200
Power nonresidues, 270
Primality testing, 55–63
Prime asymptotic density, 221
Prime density, 219, 276
Prime ideal, 224, 225
Prime number theorem (PNT), 220–224, 259
Primitive divisor of an integer sequence, 93, 206
Primitive element, 225
Primitive prime maximal divisor, 275
Proper division of a second-order linear recurrence, 246
Proper divisor of an integer, 53
Public-key cryptography, 72–74, 86, 177, 179
Pythagorean formula, 15

Quadratic congruence, 67

R-sequence, 206
Ramification index, 225
Rank exponent of a prime, 30
Rank of appearance, 26
Rank of appearance of an impulse sequence, 189
Rank of maximal division, 252
Recursion formula, 12
Regular Lucas sequences, 13
Regular prime, 26
Regularly divisible sequence, 134
Resultant, 206
RIC (recursion plus initial conditions), 15, 16, 21
Roettger's sequences, 177–179, 211

Sequence, 1

w-density, 221
Wolstenholme congruence, 274

Name Index

Abouzaid, M., 160
Abrate, M., 207
Adams, J., 281
Adams, W., 170
Aggarwal, D., 74
Agrawal, M., 62
Alaca, Ş., 262
Amato, P., 102
Anderson, P., 241
André, C., 282
Andrews, G., 152, 157
Anglin, W. S., 282
Aoki, M., 262
Apostol, T. M., 262
Atkin, O., 62
Aurifeuille, L-.F-.A., 89
Autebert, J.-M., 289
Azose, J., 160

Bézivin, J.-P., 207, 263
Babbage, C., 151
Bach, E., 70
Bachet, C.-G., 288
Bailey, D. F., 152
Baillie, R., 70
Baker, A., 273
Bala, P., 214
Ballot, C., 12, 132, 155, 156, 158, 168, 173, 176, 189, 240, 248, 273, 275
Barbeau, E. J., 71
Barbero, S., 207, 216
Bateman, P., 100, 287
Bavencoffe, E., 263
Bell, E. T., 169, 173, 174, 187, 200, 201, 287
Benford, F., 223
Benjamin, A., 119
Bennett, C., 161
Berger, A., 263
Berrizbeitia, P., 59, 62
Berry, T., 59, 62
Bicknell-Johnson, M., 288
Bilharz, H., 260
Bilu, Y., 97
Bleichenbacher, D., 73
Boneh, D., 73, 74
Bosma, W., 59
Boyron, M., 282
Brünnow, F., 282
Brandner, G., 86
Bressoud, D., 5
Bright, C., 187
Brillhart, J., 12, 60, 62, 90, 287
Bruckman, P., 241
Brun, V., 153, 155, 157
Buchmann, J., 72
Bugeaud, Y., 72
Burr, S., 98

Cailler, C., 67
Caldwell, C., 100
Carlitz, L., 116, 128
Carmichael, R. D., 11, 55, 59, 187, 287
Carrillo, J., 161
Cassini, G. D., 2
Catalan, E., 170
Cauchy, A.-L., 231
Cebotarev, N., 219, 223, 224, 226, 228, 230, 260, 261
Cerutti, U., 216
Chen, X., 161
Cipolla, M., 66, 177
Cohn, J. H. E., 72
Cox, D. A., 62
Crandall, R., 5, 58

Décaillot, A.-M., 170, 279, 283, 285
Davenport, H., 260
Davison, T. M. K., vii
de Kooning, W., 79
de la Vallée Poussin, C.-J., 220
de Looij, R., 204

© Springer Nature Switzerland AG 2023

C. J.-C. Ballot, H. C. Williams, *The Lucas Sequences*, CMS/CAIMS Books in Mathematics 8, https://doi.org/10.1007/978-3-031-37238-4

de Sautoy, M., 11
Debellevue, M., 146
Delannoy, H., 169
Deng, Y., 59
Devlin, K., 2
Dickson, L. E., 71
Dietzfelbinger, M., 62
Dipra, M., 91
Dirichlet, P. G. L., 224
Durfee, G., 74

Einstein, A., 79
Ekhad, S., 161
Elia, M., 160
Engstrom, H. T., 187
Erdős, P., 287
Euclid, 54
Euler, L., 3, 54, 115
Everest, G., 187, 208, 263

Fürlinger, J., 161
Fermat, P., 4, 22, 55, 168, 169
Feynman, R., 267
Fibonacci, 2
Fiduccia, C. M., 188
Fine, N. J., 142
Flammarion, C., 281
Fontené, G., 107
Franke, J., 62
Fray, R. D., 143
Freitas, G., 161
Frobenius, F. G., 223, 230, 231
Fuchs, A., 263

Gallagher, P. X., 263
Gand, É., 281
Garnier, J., 279
Gauss, C. F., 106
Genaille, H., 283
Genocchi, A., 4, 55
Germain, S., 100, 105
Gilson, B. R., 2
Glaisher, J. W. L., 161
Goldberg, S., 172
Goldstein, C., 290
Gould, H. W., 113, 127
Graham, R., 162
Graham, R. L., 287
Grantham, R. L., 170
Granville, A., 30, 62, 272, 287
Grosslight, J., 54
Grothendieck, A., 267
Gurovski, A., 91
Guy, R., 210, 212, 245
Guy, R. K., 70

Hadamard, J., 220
Hajdu, L., 6
Hall, Jr., M., 172, 205, 271
Hambleton, S., 175
Hanrot, G., 102, 161
Hardy, G. H., 12, 158
Hardy, K., 177
Harkin, D., 201, 286, 287
Harrison, J., 53
Hasse, H., 8
Hill, T., 263
Hofbauer, J., 161
Hoggatt, Jr., V. E., 162
Holte, J. M., 143, 149
Hooley, C., 242
Horn, R., 100
Hu, H., 144, 150, 157
Huang, D., 59

Ibrahimpašić, B., 73
Ieronymou, E., 162
Ireland, K., 62

Jacobi, C. G. J., 168, 200
Jacobson, Jr., M. J., 71
Jarden, D., 90, 115, 116

Křížek, M., 99, 101
Kayal, N., 62
Kaye, P., 73
Kida, M., 262
Killpatrick, K., 120
Kimball, W., 152, 153
Kiss, P., 245
Klavžar, S., 290
Kleinjung, T., 76

Knuth, D. E., 134
Konvalina, J., 123
Koshkin, S., 205, 214, 216
Koshy, T., 2
Kovalevskaya, S., 219
Kronecker, L., 223, 230
Kryuchkova, E., 146
Kummer, E., 133

Laflamme, R., 76
Lagarias, J., viii, 8, 36, 287
Lagrange, J.-L., 4
Laisant, C.-A., 169, 173, 177, 179, 285, 286
Lamé, G., 3
Launay, M., 264
Laxton, R., 157
Le Lasseur, H., 89
Le Verrier, U., 280, 281
Legendre, A.-M., 4, 66
Lehman, I., 2
Lehmer, D. H., 11, 58, 59, 62, 66, 71, 268, 287
Lehmer, D. N., 12, 287
Lehmer, E., 287
Lemoine, É., 169
Lenstra, A. K., 69
Lenstra, Jr., H. W., 72
Letta, G., 263
Leudesdorf, C., 158
Li, H.-C., 101
Libri, G., 2
Lidl, R., 65, 85
Liouville, J., 287
Ljujić, Ž., 240
Ljunggren, W., 72
Lombaers, P., 163
Longchamps, G. A., 177
Lopes, J., 161
Loxton, J., 177
Luca, F., 263, 275
Lucas, É., 3, 11, 12, 19, 20, 28, 29, 55–58, 107, 142, 165, 166, 168–174, 177–179, 183, 192, 279, 280

Müller, S., 67, 69, 74, 173, 178
Müller, W. B., 86
Mátyás, F., 245
Machacek, J., 161
MacMahon, P., 129
Makraduli, J., 102
Marcus, D., 264
Marques, D., 140
Martin, G., 263
Matijasevitch, Y., 35
Matiyasevich, Y., 245
Maurer, U. M., 73, 74
McIntosh, R., 91, 270
Meštrović, R., 142, 152
Mendelsohn, N. S., 173
Menezes, A. J., 72
Mersenne, M., 54
Mignotte, M., 72
Miller, J. C. P., 188
Mirzakhami, M., 165
Monogan, M., 30
Montgomery, P., 70
Montgomery, P. L., 90
Morain, F., 62, 76
Mordell, L. J., 71
Moree, P., 40, 240, 242, 258
Morton, P., 264
Mosca, M., 76
Motzkin, T., 115
Moutard, T. F., 167
Mullen, G. L., 85
Murata, L., 223, 260, 261
Murru, N., 216

Nöbauer, W., 86
Nagell, T., 175
Narkiewicz, W., 264
Newton, I., 199
Niederreiter, H., 65, 85

Ochem, P., 54
Odlyzko, A., 287
Offenbach, J., 285
Ohtsuka, H., 156
Olive, G., 143
Oosterhout, A. D., 208, 215

Pólya, G., 128
Pan, H., 157
Panario, D., 85
Pappalardi, F., 240
Pascal, B., 288
Pasteur, L., 279, 280
Patashnik, O., 162
Pethö, A., 207
Petr, C., 290
Phunphayap, P., 139
Pierce, T. A., 209
Pinch, R., 251
Pleasants, P., 102
Plott, S., 119
Pocklington, H. C., 177
Pollard, H., 265
Pollard, J. M., 70
Pomerance, C., 5, 58, 63, 131, 287
Poncelet, J.-V., 167
Pongsriiam, P., 139
Posamentier, A. S., 2
Prachar, K., 265
Proust, M., 105
Puri, Y., 2

Quinn, J., 161

Ramanujan, S., 287
Rao, M., 54
Rao, N. R., 151
Reiland, E., 161
Renaud, H., 291
Ribenboim, P., 5, 12, 287
Riesel, H., 88
Robinson, D. W., 187
Robinson, R., 12, 61
Roettger, E., 57, 59, 62, 90, 165, 178, 179, 208, 210, 211, 215, 270
Rosen, J., 163
Rosen, M., 62
Roskam, H., 258
Rostand, J., 183
Rotman, J. J., 231
Rovelli, C., 1
Rudman, R., 175

Sagan, B., 119, 120
Sagan, C., 11
Said, M. R., 177
Sakai, Y., 262
Savage, C., 119, 120
Saxena, N., 62
Schinzel, A., 101, 265
Schmid, B., 73
Schmidt, W. M., 71
Schwartz, L., 267
Schwer, S. R., 289
Selfridge, J. L., 62, 287
Sellers, J., 163
Serre, J.-P., 224, 237
Serret, J. A., 167
Shah, A., 98
Shallit, J. O., 69, 70
Shallue, A., 91, 103
Shanks, D., 66, 170, 243
Shapiro, H., 103
Shawe-Taylor, J., 73
Shi, L.-L., 155
Shipsey, R., 204
Shorey, T. N., 71
Shparlinski, I., 197, 263
Sierpiński, W., 8
Siksek, S., 72
Silverman, J., 203, 204
Silverman, R., 90
Singh, P., 2
Sloane, N. J. A., 217
Smart, N., 71
Smith, D. E., 169
Smith, P., 73
Somer, L., 99, 101, 265
Southwick, J., 146
Spencer-Brown, D. J., 188
Stange, K., 204
Stanley, R., 152
Stark, H., 287
Stein, A., 62
Stender, H.-J., 175
Stephens, N., 203
Steuding, J., 71
Stevenhagen, P., 240, 242

Stinson, D. R., 72
Sun, Z.-W., 144, 157
Suwa, N., 254
Swart, C., 204
Sylvester, J. J., 64
Szekeres, G., 170
Szikszai, M., 6
Słota, D., 83

Tauraso, R., 156
Tijdeman, R., 71
Tonelli, 66
Trojovský, P., 163
Turnwald, G., 102
Twain, M., 1, 279

Vajda, S., 2, 3
van der Poorten, A. J., 197, 207, 208, 263
van der Waerden, B. L., 266
Venkatesan, R., 74
Vinson, J., 164
Voutier, P., 102

Wagon, S., 5
Wagstaff, Jr., S. S., 69
Wang-Wei, 219
Ward, M., 8, 97, 107, 115, 134, 157, 172, 173, 184, 187, 201–204, 206, 220, 234–237, 242, 246, 251, 287
Ward, T., 2, 216, 263
Waring, E., 151
Watson, G. N., 282
Weaver, J., 120
Webb, W., 152, 153
Webster, J., 91
Weierstrass, K., 219
Weintraub, S., 88
Wells, D. L., 143
Wieferich, A., 30
Wiertelak, K., 240
Wilf, H., 134
Williams, H. C., 3, 5, 12, 57, 61, 62, 68–71, 73, 90, 91, 100, 175–177, 179, 191, 210–212, 215, 270, 288
Williams, K. S., 177, 262
Wilson, B., 143
Wirth, T., 76
Wituła, R., 83
Wolstenholme, J., 6, 151, 273
Wright, E. M., 12

Yabuta, M., 94